E-Lins WAP100 Series AP

User Manual

E-Lins Technology Co., Ltd

ADDRESS: Bld22., Longxi Garden, Nonglin RD., Futian District, Shenzhen, 518000, China

PHONE: 86-755-83700465

WEB: http://www.szelins.com

Contents

Release Notes:

- Release 1.0 This is the first Release

1 Product overview

1.1 Introduction

The high-performance Wireless Network Access Point (AP) is designed for enterprise and public access applications. Embedded with the Atheros chipset, it boasts network robustness, stability and wider network coverage. Based on 802.11n (Draft 2.0), the access point supports high-speed data transmission of up to 300Mbps.

The access point is capable of operating in different modes, which makes it suitable for a wide variety of wireless applications, including long-distance deployments.

Designed with dual polarization high gain antenna it offers a compact, rugged design for outdoor installation and excellent performance.

Moreover, its integrated Power over Ethernet (PoE) allows the access point to be used in areas where power outlets are not readily available.

To protect your security and privacy, the access point is armed with many enhanced and latest wireless security features such as IEEE 802.11i standards, MAC Address Filtering, IEEE 802.1x Authentication and 64/128-bit WEP (Wired Equivalent Privacy) to ensure privacy for the heterogeneous mix of users within the same wireless network.

The access point also incorporates a unique set of advanced features such as: Virtual AP to deliver multiple services; Long-Range parameter fine-tuning which provide the access point with the ability to auto-calculate parameters such as slot time, ACK time-out and CTS time-out to achieve a longer range.

1.2 Features and benefits

- **Point-to-Point & Point-to-MultiPoint Support**

Point-to-Point and Point-to-MultiPoint communication between different buildings enables you to bridge wireless clients that are kilometres apart while unifying the networks.

- **Virtual AP (Multiple SSID)**

Virtual AP implements mSSID (Multi-SSID) This allows a single wireless card to be set up with multiple virtual AP connections with different SSIDs or BSSID (Basic Service Set Identifier) and security modes.

- **Highly Secured Wireless Network**

The access point supports the highest available wireless security standard: IEEE802.11i compliant. The access point also supports IEEE 802.1x for secure and centralized user-based authentication. Wireless clients are thus required to authenticate through highly secure methods like EAP-TLS, EAP-TTLS, and EAP-PEAP, in order to obtain access to the network.

- **uConfig Utility**

The exclusive uConfig utility allows users to access the user-friendlyWeb configuration interface of the access point without having to change the TCP/IP setup of the workstation.

- **HTTPS**

The access point supports HTTPS (SSL) in addition to the standard HTTP. HTTPS (SSL) features additional authentication and encryption for secure communication.

- **Telnet**

Telnet allows a computer to remotely connect to the access point CLI (Command Line Interface) for control and monitoring.

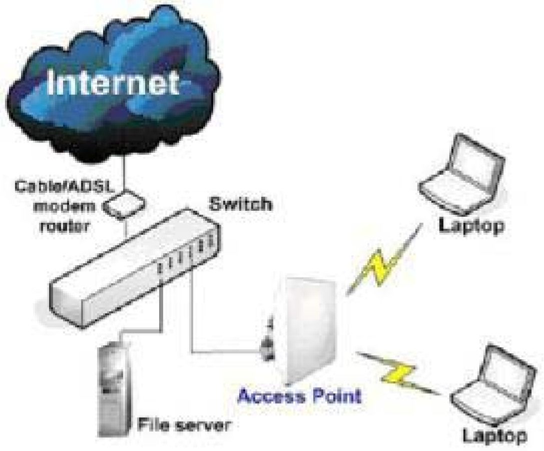
- **SSH**

SSH (Secure Shell Host) establishes a secure host connection to the access point CLI for control and monitoring.

1.3 Operation Modes and Connection Examples

1.3.1 Access Point and Access Point WDS Mode

The Access Point Mode is the default mode of the device. It enables the bridging of wireless clients to wired network infrastructure and enables transparent access and communication with each other. The illustration belowshows a typical resources sharing application example using this device. The wireless users are able to access the file server connected to the switch, through the access point in Access Point Mode.



1.3.2 Access Point WDS Mode

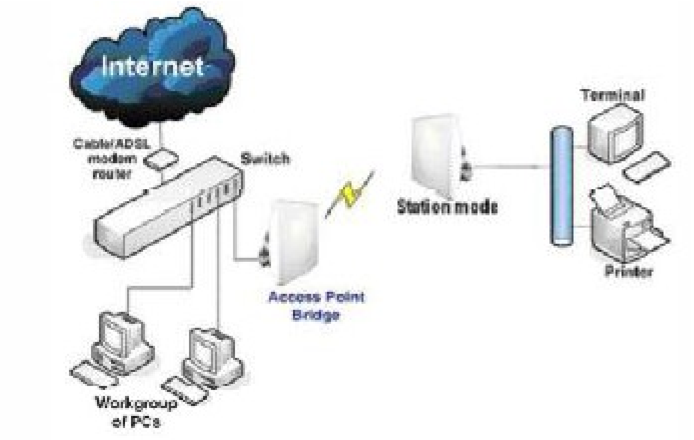
This ismode is generally use for point-to-point or point-to-multi-point connection.

It is mainly use with StationWDS to build the point and multi-point connections.

1.3.3 Station Mode

In **Station** mode the device acts as a wireless client.When connected to an access point, it creates a network link between the Ethernet network connected at this client device, and the wireless Ethernet network connected at the access point.

In this example the workgroup PCs on the ethernet network connected to the Station device can access the printer across the wireless connection to the access point where the printer is connected.



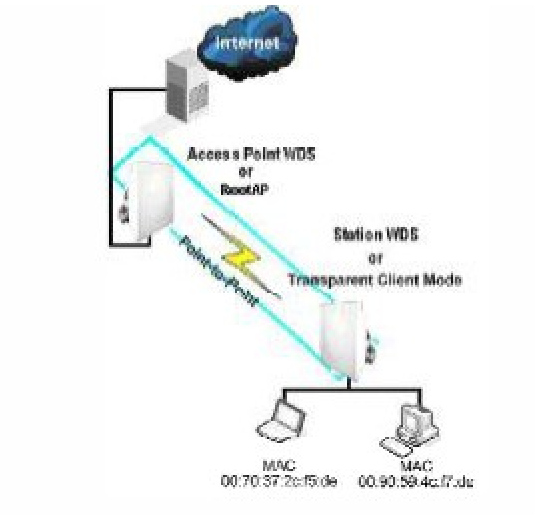
1.3.4 Station WDS Mode

StationWDS mode is similar to Station mode. The difference is StationWDS must connect to access point configured to Access Point WDS (or RootAP) mode.

StationWDS is mainly use for point-to point connection between 2 buildings or locations as far as several kilometer away.

Point to-Point	Point to-MultiPoint
An access point setup as Access Point WDS (or RootAP) and other as Station WDS (Transparent Client).	An access point setup as Access Point WDS (or RootAP) and several other devices as Station WDS (or Transparent Client).

This mode is generally used for outdoor connections over long distances, or for indoor connections between local networks.


Internet
Access Point WDS or RootAP
Station WDS or Transparent Client Mode
Point-to-Point
MAC 00:70:37:2c:f5:de
MAC 00:90:59:4c:f7:dc

1.3.5 Router Mode

In Router Mode, the device also operates as a router.

Either the wireless or Ethernet can be setup as WAN connection to a broadband modem. Wireless as WAN is known as **Station + Router mode** (or **Wireless Routing Client** mode) and Ethernet as WAN is known as **AP + Router mode** (or **Gateway** mode). Device supports several types of broadband connections Static IP, Dynamic IP and PPPoE. For setup details refer to the respective section.

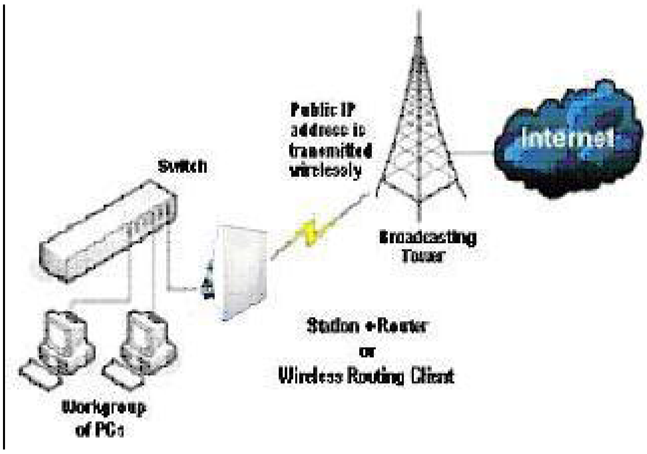
The illustration below shows the Ethernet port is setup as theWAN port and the wireless connection as the LAN.

Station + Router connection example

Wireless is use to connect to the broadband.

Ethernet is the local network (LAN)

sharing the broadband connection.

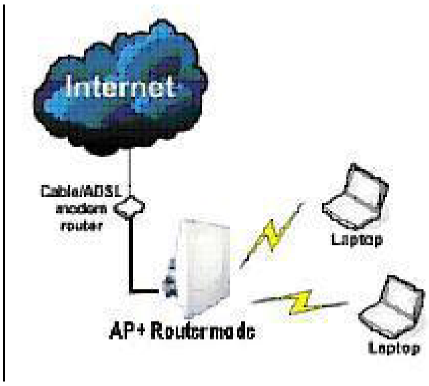


AP + Router connection example

Ethernet is use to connect to the broadband.

Wireless is the local network (LAN)

sharing the broadband connection.



Broadband Internet Access Type:

Static IP Address

Use Static IP Address you have subscribed a fixed IP or range IP addresses fromyour ISP.

Dynamic IP Address

With Dynamic IP Address the device automatically request IP address frommodemor ISP.

PPP over Ethernet (PPPoE)

When using ADSL services provided by your ISP support PPPoE connection.

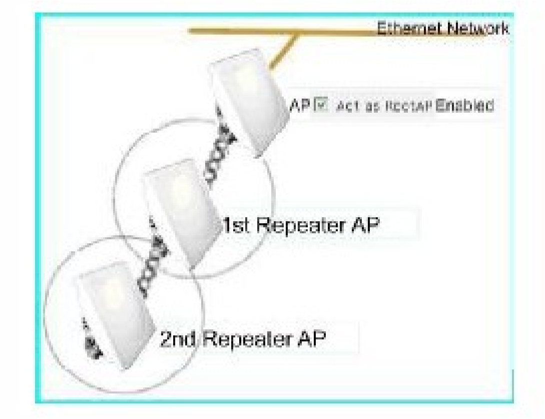
1.3.6 Repeater WDS Mode

Repeater WDS Mode to mainly to extend the wireless range and coverage of the wireless network allowing access and communications over places generally difficult for wireless clients to connect to the network.

In Repeater mode, the access point acts as a relay for network signals on the network by regenerating the signals it receives, and retransmitting themto main network infrastructure.

Detailed information on the Repeater mode is available in the Repeater Setup section.

**** Note: Repeater WDS requires the access point to be setup in RootAP or Access Point WDS mode to work.**



2 Installation

2.1 Setup requirements

Before starting, please verify that the following is available:

- CAT5/5e networking cable
- At least 1 computer installed with a web browser and a wired or wireless network interface adapter.
- All network nodes installed with TCP/IP and properly configured IP address parameters.

2.2 Hardware installation

The access point can be powered using the 802.3af standard PoE Injector. This accessory supplies operational power to the wireless access point via the Ethernet cable connection.

Step 1: Use an RJ45 Ethernet cable to connect one end of the cable to the Ethernet socket of the Injector and the other end to one of the LAN ports of the accesspoint.

Warning:

When one port is used for PoE, the other port cannot connect to any other network device.

Step 2: Next, connect the RJ45 Ethernet cable attached to the standard PoE Injector to your PC s Ethernet network adapter.

Once you have finished configuring your access point, you can connect thePoE Injector s RJ45 Ethernet cable to your network device, such as to a switchor hub.

2.3 Configure the IP Address

After setting up the hardware you need to assign an IP address to your PC so that it is in the same subnet as the access point.

2.3.1 For Windows 95/98/98SE/ME/NT

Step 1:

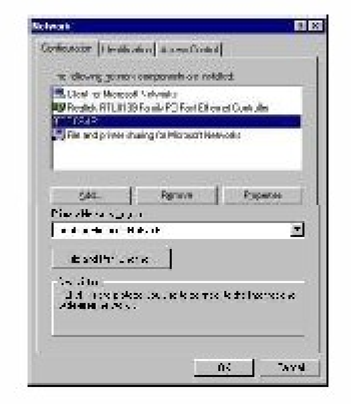
From your desktop, right-click the **Network Neighborhood** icon and select **Properties**.

Step 2:

Select the network adapter that you are using, then right-click and select Properties.

Step 3:

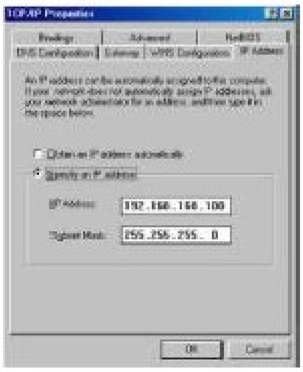
Highlight **TCP/IP** and click on the **Properties** button.



Step 4:

Select the **Specify an IP address** radio button.

Set the IP address to 192.168.168.X and Subnet mask to 255.255.255.0, where X can be any number from 2 to 254.



○ Obtain an IP address automatically
● Specify an IP address

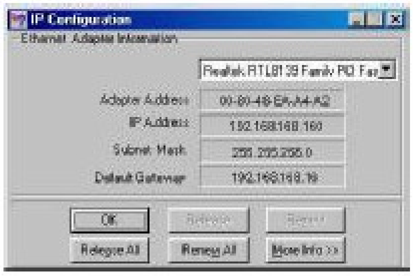
IP Address: 192.168.168.100

Subnet Mask: 255.255.255.0

Step 5:

To verify that the IP address has been correctly assigned to your PC, go to the **Start** menu, select **Run**, and enter the command: winipcfg.

Select the Ethernet adapter fromthe drop-down list and click **OK**.



Realtek RTL8139 Family PCI Fas

Adapter Address: 00-80-48-E?-A4-A2

IP Address: 192.168.168.160

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.168.18

PC is now setup with proper IP address to communicate with the access point.

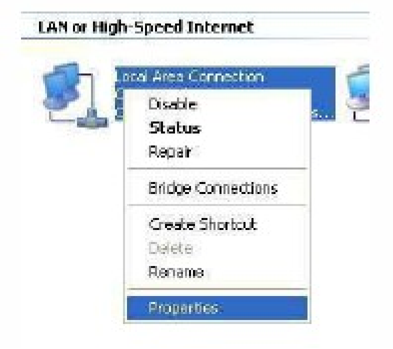
2.3.2 For Windows XP/2000

Step 1:

Go to your desktop, right-click on the **My Network Places** icon and select **Properties**.

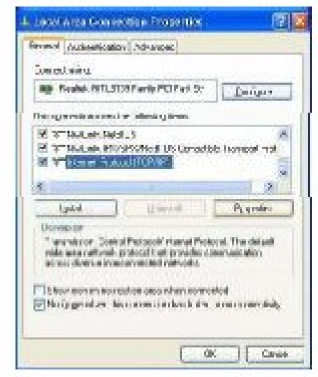
Step 2:

Right-click the network adapter icon and select **Properties.**



Step 3:

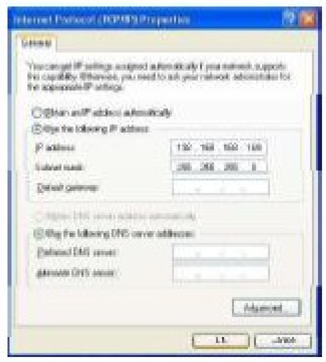
Highlight **Internet Protocol (TCP/IP)** and click on the **Properties** button.



Step 4:

Select the **Use the following IP address** radio button.

Set the IP address to 192.168.168.X and subnet mask to 255.255.255.0, where X can be any number from 2 to 254.

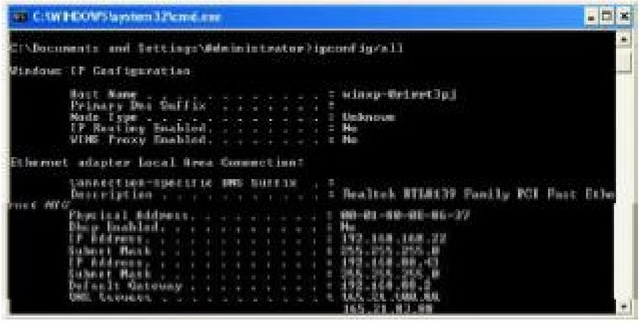


Step 5:

Click on the **OK** button to close all windows.

Step 6:

To verify that the IP address has been correctly assigned to your PC, go to the **Start** menu, **Accessories**, select **Command Prompt**, and type the command: *ipconfig/all*



C:\WINDOWS\system32\cmd.exe

```
C:\Documents and Settings\Administrator>ipconfig/all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : winxp-Wrleet3pj
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Realtek RTL8139 Family PCI Fast Ethe
rnet NIC
        Physical Address. . . . . . . . . : 00-01-00-0E-06-37
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.168.22
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : 192.168.88.43
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.88.2
        DNS Servers . . . . . . . . . . . : 165.21.100.88
                                            165.21.83.88
```

PC is now setup with a proper IP address to communicate with the access point.

3 Access the Web Interface

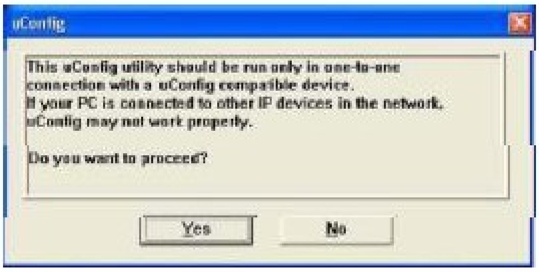
There are two methods to access to the web-based Interface of your access point:

3.1 Through our Utility uConfig

You can access to the web-based interface directly without the need to assign a different IP address to your PC.

Step 1: install the **uConfig** utility to your hard disk.

Step 2: After installation double-click on the **uConfig** icon and click on the **Yes** button.



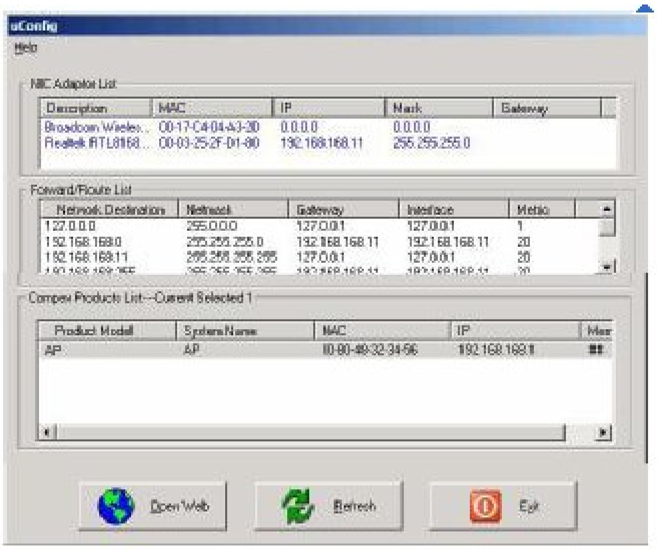
uConfig

This uConfig utility should be run only in one-to-one connection with a uConfig compatible device.
If your PC is connected to other IP devices in the network, uConfig may not work properly.

Do you want to proceed?

Step 3: Select the access point from the products list and click on the **Open Web** button.

To retrieve and display the latest device(s) in the list, click on the **Refresh** button.



uConfig

NIC Adaptor List

Description	MAC	IP	Mask	Gateway
Broadcom Wireles...	00-17-C4-04-A3-20	0.0.0.0	0.0.0.0	
Realtek RTL8168...	00-03-25-2F-D1-80	192.168.168.11	255.255.255.0	

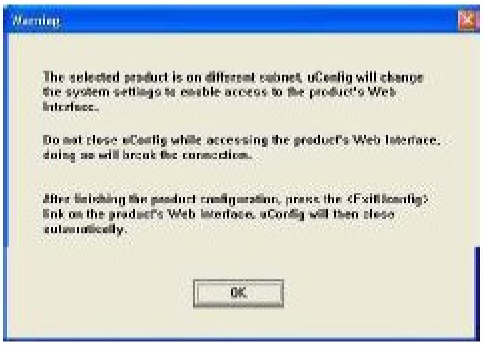
Forward/Route List

Network Destination	Netmask	Gateway	Interface	Metric
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.168.0	255.255.255.0	192.168.168.11	192.168.168.11	20
192.168.168.11	255.255.255.255	127.0.0.1	127.0.0.1	20
192.168.168.255	255.255.255.255	192.168.168.11	192.168.168.11	20

Compex Products List---Current Selected 1

Product Model	System Name	MAC	IP	Mas
AP	AP	00-80-48-32-34-56	192.168.168.1	##

Step 4: Do not exit the uConfig program while accessing the web-based interface as this will disconnect you from the device. Click on the **OK** button.


Warning

The selected product is on different subnet, uConfig will change the system settings to enable access to the product's Web Interface.

Do not close uConfig while accessing the product's Web Interface, doing so will break the connection.

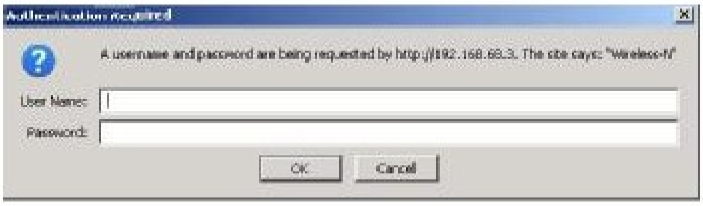
After finishing the product configuration, press the <ExituConfig> link on the product's Web Interface, uConfig will then close automatically.

Step 5: At the login prompt, enter the User Name and Password.

The default are :

User Name : **admin**

Password : **password**

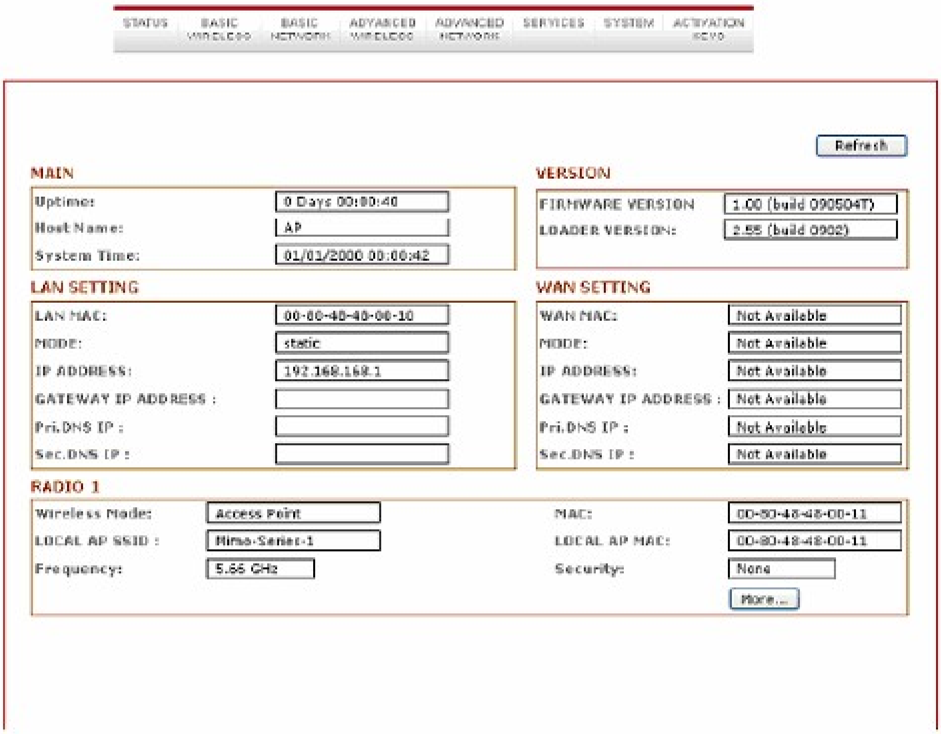

Authentication Required

A username and password are being requested by http://192.168.68.3. The site says: "Wireless-N"

User Name:

Password:

Step 6: It then opens the device home page. The Status page.



MAIN

Uptime: 0 Days 00:00:40

Host Name: AP

System Time: 01/01/2000 00:00:42

VERSION

FIRMWARE VERSION 1.00 (build 090504T)

LOADER VERSION: 2.55 (build 0902)

LAN SETTING

LAN MAC: 00-80-48-48-00-10

MODE: static

IP ADDRESS: 192.168.168.1

GATEWAY IP ADDRESS :

Pri.DNS IP :

Sec.DNS IP :

WAN SETTING

WAN MAC: Not Available

MODE: Not Available

IP ADDRESS: Not Available

GATEWAY IP ADDRESS : Not Available

Pri.DNS IP : Not Available

Sec.DNS IP : Not Available

RADIO 1

Wireless Mode: Access Point

LOCAL AP SSID : Mimo-Series-1

Frequency: 5.66 GHz

MAC: 00-80-48-48-00-11

LOCAL AP MAC: 00-80-48-48-00-11

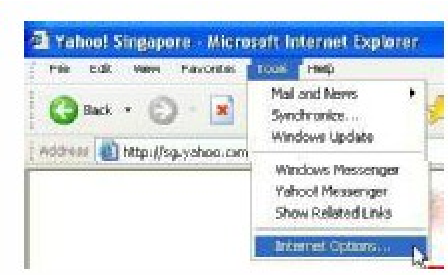
Security: None

3.2 Access with a Web Browser

Step 1:

Launch your Web browser. e.g. MS Internet Explorer, FireFox, Netscape, etc..

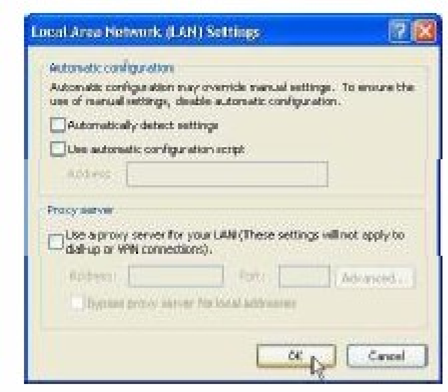
For MS IE, under the Tools tab, select Internet Options.



Step 2:

Open the Connections tab and in the LAN Settings section disable all the option boxes.

Click on the OK button to update the changes.


Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☐ Automatically detect settings

☐ Use automatic configuration script

Address:

Proxy server

☐ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port: Advanced...

☐ Bypass proxy server for local addresses

Step 3:

At the Address bar type in http://192.168.168.1 and press Enter on your keyboard.

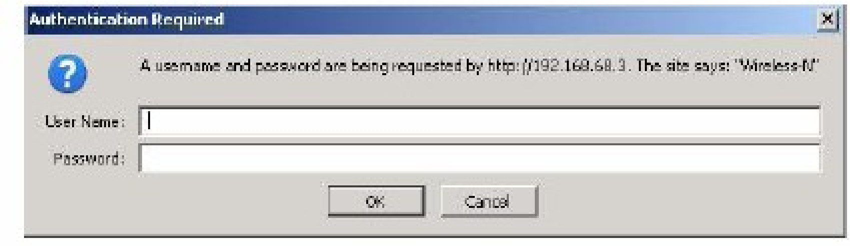
Step 4:

At the login prompt, enter the User Name and Password.

The default are :

User Name : **admin**

Password : **password**

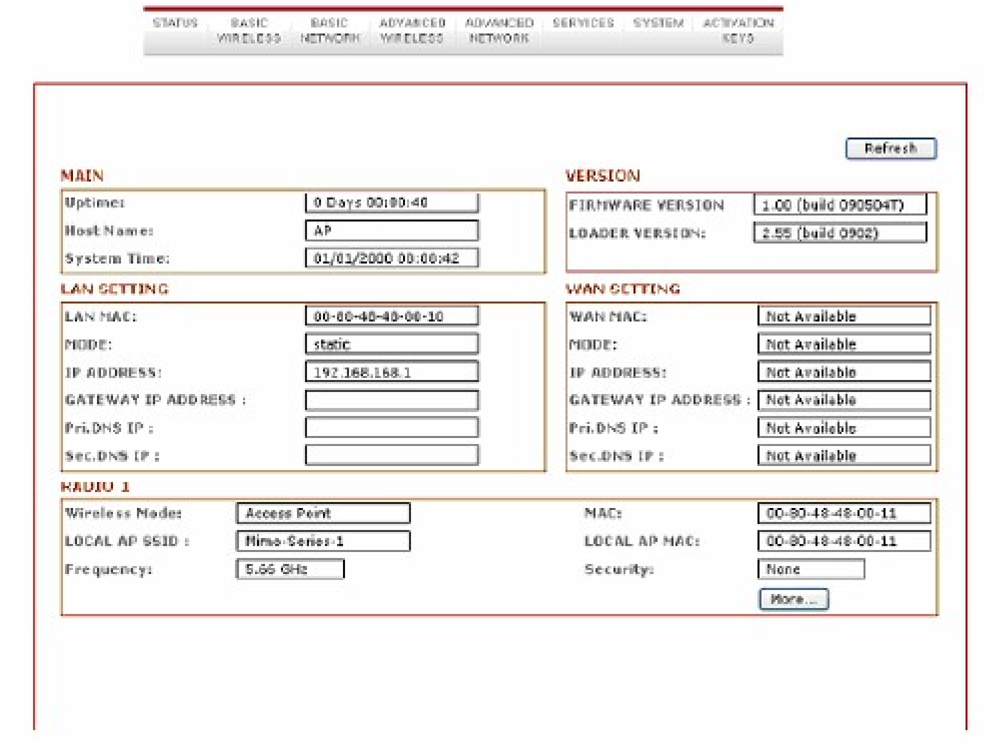

Authentication Required

A username and password are being requested by http://192.168.68.3. The site says: "Wireless-N"

User Name:

Password:

It then opens the device home page. The Status page.



MAIN

Uptime:	0 Days 00:00:40
Host Name:	AP
System Time:	01/01/2000 00:00:42

VERSION

FIRMWARE VERSION	1.00 (build 090504T)
LOADER VERSION:	2.55 (build 0902)

LAN SETTING

LAN MAC:	00-80-48-48-00-10
MODE:	static
IP ADDRESS:	192.168.168.1
GATEWAY IP ADDRESS :	
Pri.DNS IP :	
Sec.DNS IP :	

WAN SETTING

WAN MAC:	Not Available
MODE:	Not Available
IP ADDRESS:	Not Available
GATEWAY IP ADDRESS :	Not Available
Pri.DNS IP :	Not Available
Sec.DNS IP :	Not Available

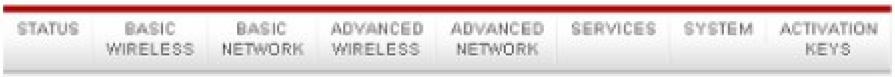
RADIO 1

Wireless Mode:	Access Point	MAC:	00-80-48-48-00-11
LOCAL AP SSID :	Mimo-Series-1	LOCAL AP MAC:	00-80-48-48-00-11
Frequency:	5.66 GHz	Security:	None

4 Navigation

4.1 Main Menu

4.1.1 Main Menu Bar



Status : Page displays current status of the device and the statistical information.

Basic Wireless : Page contains the controls for a wireless network configuration, while covering basic wireless settings which define operating mode, associating details and data security options.

Basic Network : Page covers the configuration of network operating mode, IP settings and network services (i.e. DHCP Server).

Advanced Wireless : Page settings for more advanced wireless features. Advanced Network page settings for more advanced network features.

Services : Page covers the configuration of system management services (i.e. Ping Watchdog, Auto-Reboot, SNMP, NTP, Telnet, SSH, SystemLog).

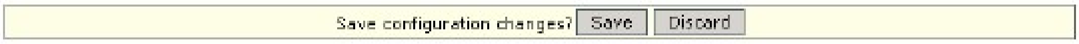
System : Page contains controls for system maintenance routines, administrator account management, device customization and configuration backup.

Activation Keys : Optional special add-on functions you can purchased separately to activate in device.

4.1.2 How to save changes.

After made changes fromeach respective setup page, click this button, Apply Settings

Next the prompt below appear. You are asked to confirm if you want to save the change permanently to device flash.

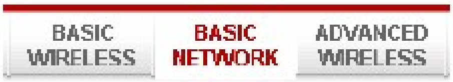

Save configuration changes? Save Discard

Click Save will write all configuration changes to flash.

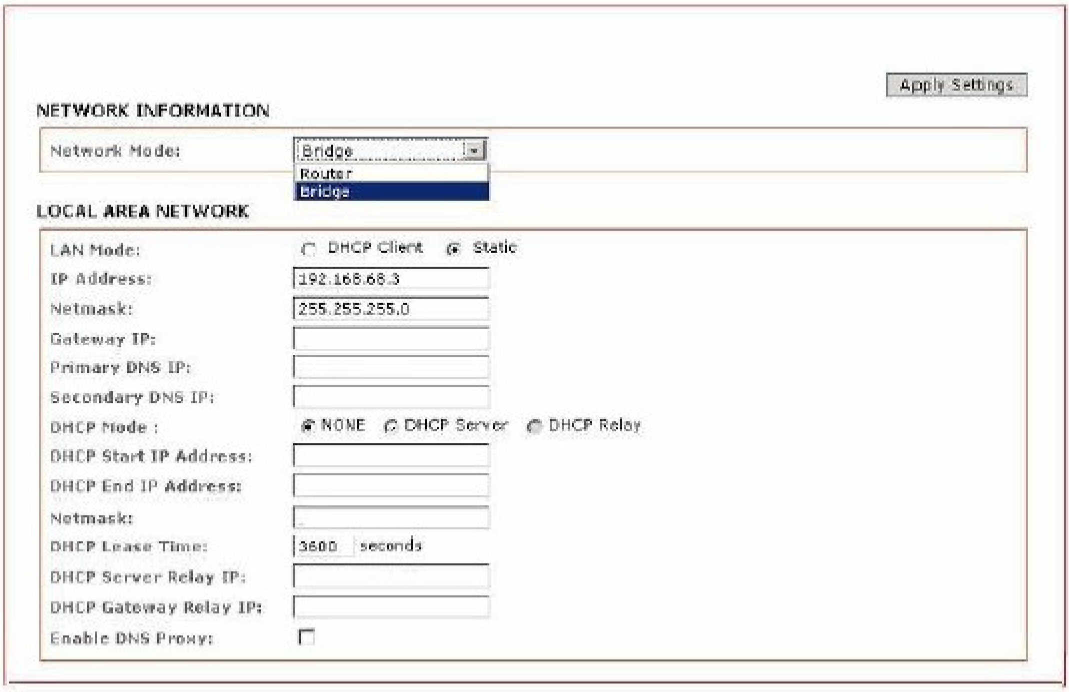
Click Discard will discard all changes made.

If not sure what changes were made earlier, recommend to discard and reconfigure again.

4.2 Basic Network Tab



Click **BASIC NETWORK** fromthe menu bar to open the page as show below.



NETWORK INFORMATION

Network Mode: Bridge (Router / Bridge)

LOCAL AREA NETWORK

LAN Mode:	○ DHCP Client ● Static
IP Address:	192.168.68.3
Netmask:	255.255.255.0
Gateway IP:	
Primary DNS IP:	
Secondary DNS IP:	
DHCP Mode :	● NONE ○ DHCP Server ○ DHCP Relay
DHCP Start IP Address:	
DHCP End IP Address:	
Netmask:	
DHCP Lease Time:	3600 seconds
DHCP Server Relay IP:	
DHCP Gateway Relay IP:	
Enable DNS Proxy:	□

4.2.1 Network Modes: Bridging and Routing

Network Mode:

Select between Bridge (default) and Router mode.

4.2.2 LAN Setup

LAN Mode:

Static: (default) lets you enter a specific IP address for the device.

Default IP address is 192.168.168.1

DHCP Client: when set let device learn the IP address automatically fromthe network.

Netmask:

Let you set the class for the IP address set.

Default classC and value is 255.255.255.0

Gateway: (optional)

Enter the gateway IP address of the network the device is connected.

Primary DNS IP: (optional)

Enter the primary DNS IP address nearest to the gateway router.

Secondary DNS IP: (optional)

Enter the secondary DNS IP address nearest to the gateway router.

DHCP Mode:

None: function disabled

DHCP Server: Check to enable. Device act IP address distribution server automatically issue IP address and other network information to the DHCP Client request them.

DHCP Relay: check to enable. Enter the IP address of the remote DHCP server where the DHCP Client request will be relayed to.

DHCP Start IP Address:

Enter the starting IP address to be issue.

DHCP End IP Address:

Enter the last IP address the server will issue.

Netmask:

Let you set the IP class for the IP address range set for the start and end address.

*** Note:-** if device is also the router then IP class must be same as device IP class.

DHCP Lease Time: (default is **3600** seconds or 1hour)

Enter the newlease time in seconds.

DHCP Server Relay IP:

Enter the IP address of the remote DHCP server where the DHCP Client request will be relay to get the IP address.

DHCP Gateway Relay IP:

Enter the IP address of the remote gateway where the DHCP Client request will be relay to get the gateway IP address.

Enable DNS Proxy:

Check to enable function. Device router operation will act as proxy to resolve all DNS requests.

4.3 Basic Wireless Tab

Under the tab, there is the selection of 4 radios.

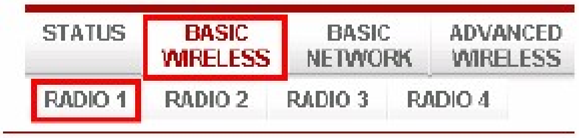


Fig 2.1 Basic Wireless Tab

Currently device support only one 802..11n radio card. Select **RADIO 1** to configure. BasicWireless Tab contains all the wireless setup, which is necessary for the operator to setup the wireless part of the link.

Enable the radio

☑ Enable Radio 1

Fig 2.2 Enable Radio Checkbox

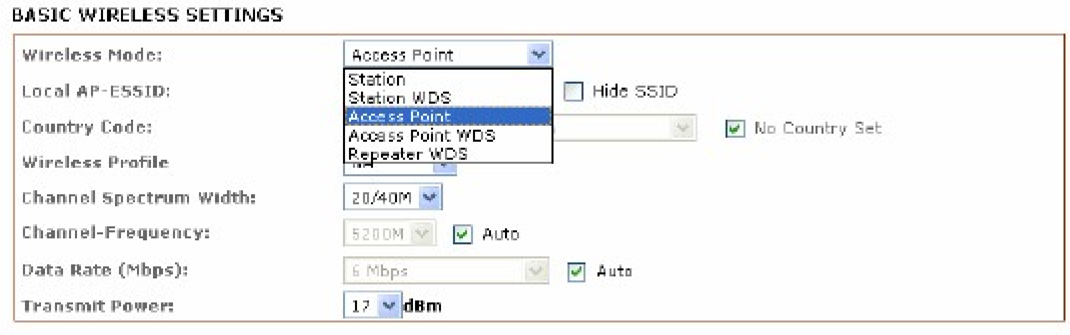
Tick/Untick the checkbox to enable/disable the radio.

4.3.1 Basic Wireless Settings

All the basic wireless settings can be configured in this page. Operators can change the ESSID, regulatory country code, wireless profile, channel spectrum width, frequency of interest, data rates, transmit power and rate aggressiveness.

Wireless Mode

There are **5 modes** available.



BASIC WIRELESS SETTINGS

Wireless Mode: Access Point

Local AP-ESSID: □ Hide SSID

Country Code: ☑ No Country Set

Wireless Profile

Channel Spectrum Width: 20/40M

Channel-Frequency: 5200M ☑ Auto

Data Rate (Mbps): 6 Mbps ☑ Auto

Transmit Power: 17 dBm

Access Point

This mode can be connected to **Station** mode, and then forwards all the traffic to the network devices connected to the Ethernet devices of the Station.

Access Point WDS

This mode can be connected to StationWDS mode. UsingWDS protocol, it allows a client or station device to bridge wireless traffic transparently.

Station:

This is a client mode that can be connected to the Access Point mode. It is used to bridge the wireless connection to an Access Point. It forwards all the traffic to/fromthe network devices to the Ethernet interface. This mode translates all the packets that pass through device to its own MAC address, thus resulting in a lack of transparency.

Station WDS:

WDS is the acronymof Wireless Distribution System. It can be connected to the **Access Point WDS** mode. It enables packet forwarding at layer 2 level. Unlike Station mode, it is fully transparent at layer 2 level.

****Note: for Station WDS, Access Point WDS, Repeater WDS:**

WDS protocol used is not defined as the standard, thus compatibility

I ssues between equipment fromdifferent vendors might arise.

Repeater WDS

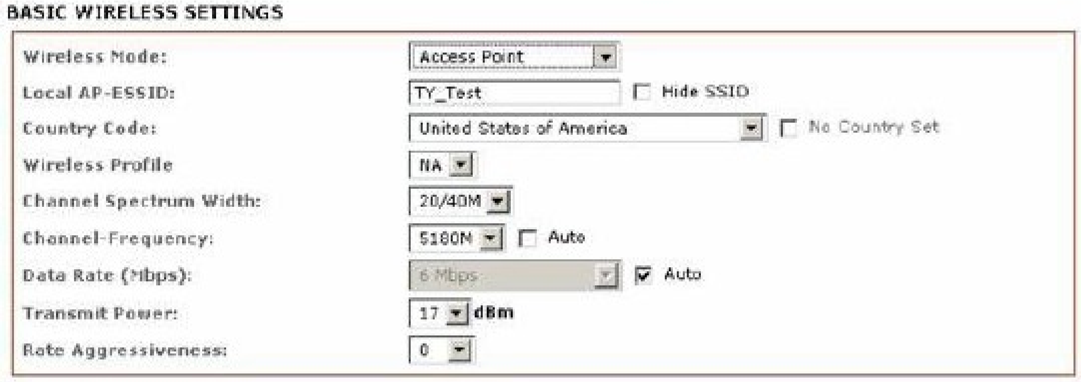
This mode consists of a StationWDS and an Access Point WDS mode. The Repeater WDS must first link up with an Access Point WDS, and then it can link up with a StationWDS. It acts as an extension to the link and can add more Repeater WDS as necessary.

***Note: for Repeater WDS:**

ESSID must be the same for the Remote AP and the Local AP.

The channels used will follow the Access Point WDS that it first linked up to.

4.3.2 Access Point Parameters Settings



BASIC WIRELESS SETTINGS

Wireless Mode:	Access Point
Local AP-ESSID:	TY_Test □ Hide SSID
Country Code:	United States of America □ No Country Set
Wireless Profile	NA
Channel Spectrum Width:	20/40M
Channel-Frequency:	5180M □ Auto
Data Rate (Mbps):	6 Mbps ☑ Auto
Transmit Power:	17 dBm
Rate Aggressiveness:	0

Fig 2.3 Basic Wireless Settings (Access Point/ Access Point WDS)

Local AP-ESSID

This is the Service Set Identifier used to identify the operators wireless LAN. It should be specified while operating in Access Point or Access Point WDS mode. All the client devices within its range will receive broadcast messages from the access point advertising this SSID.

Hide SSID*:*

Once checked, this will disable advertising the SSID of the access point in broadcast messages to wireless stations. This option is only available in Access Point, Access Point WDS and Repeater WDS mode only.

Country Code

Different countries have different power levels and also frequency selections. To ensure device operation follows regulatory compliance rules, the operator should make sure that correct country code where device will be used, is selected. The channel list, output power limits, IEEE 802.11 and Channel SpectrumWidth modes will be tuned according to the regulations of the selected country.

No Country Set*:*

Option when checked, only the frequency range are available.

11n 2.4GHz is 2412-2462MHz, 11n 5GHz is 5180-5320MHz and 5745-5825MHz.

Wireless Profile:

NA is 11n 5GHz band and represents a mixed of 802.11n and 802.11a mode.

NG is 11n 2.4GHz band and represents a mixed of 802.11n, 802.11g and 802.11b mode.

Channel SpectrumWidth

20Mrepresents the data transmitted at a bandwidth of 20MHz. 20/40MHz represents the data transmitted at either 20MHz or 40MHz. In very noisy environment it automatically fall back to 20MHz to be more resilient to the interference. In situation when auto fall back did not happened, manually changing channel spectrum width to 20MHz will to help reduce interference on the link and improve performance.

*** Note: 40MHz bandwidth is non-standard for 802.11n/g mode operation. If you experience unstable performance change Channel SpectrumWidth to 20M.**

Channel Frequency

This is frequency selection you can set for device to operate on. The frequency range available depends on the country domain you select in Country Code. For 5GHz frequency range some have DFS characteristics earmarked by regulations. Selecting one of these frequencies for operation may affect and delay of 2 minutes or more (possibly up to 10 minutes in some situations) for device to attempt to establish a connection.

Auto*:* When checked, during startup, device automatically select the least interfering channels(or frequency) for the operation.

Data Rate

Data Rates consist of both the legacy rates and the MCS (Modulation Coding Scheme Only for 802.11n) rates.

6 54Mbps are Legacy Rates

MCS0 to MCS7 are 802.11n rates, which uses only 1 stream.

MCS8 to MCS15 are 802.11n rates, which uses 2 streams.

Auto*:* The data rate selected will follow an advanced rate algorithm that takes into condition the amount of errors at the data rate and fine tune to the best data rate it can use.

Transmit Power

The maximum transmit power displayed is determined by the country code and the maximum transmit power of the miniPCI that is being used.

****Note on changing channels:***

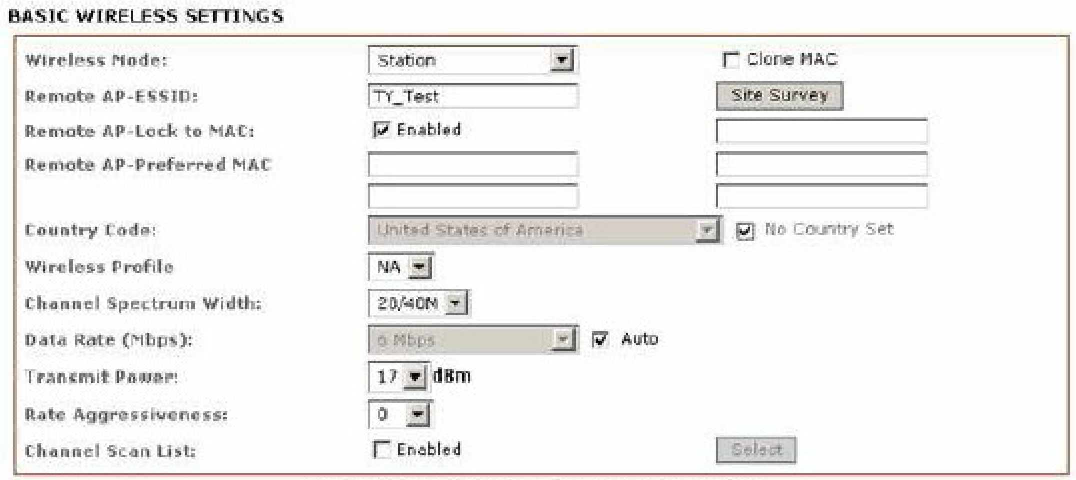
When the operator changes the channels and if this new frequency have higher power output permitted by regulation, the power previously selected low power level will remains unchanged. You need to readjust the power level to in order to take advantage higher output power available for the channel

Rate Aggressiveness

Allows user to reduce or increase transmit rate while still remain in Fully Auto Algorithm. There are 2 scenarios that Rate Aggressiveness is useful. Environment might be noisy at times. Lower the throughput will ensure better stability. Rate Aggressiveness allows device to reduce the transmit rate, so range or power can be higher. Choose a range of value from -3,-2,-1.

Environment might be free of interference. But the fully auto algorithm might give low throughput. Increase Rate Aggressiveness will increase transmit rate in this case to get higher throughput. Choose a range of value from+3, +2, +1.

4.3.3 Station Parameters Settings



BASIC WIRELESS SETTINGS

Wireless Mode: Station □ Clone MAC
Remote AP-ESSID: TY_Test
Remote AP-Lock to MAC: ☑ Enabled
Remote AP-Preferred MAC
Country Code: United States of America ☑ No Country Set
Wireless Profile: NA
Channel Spectrum Width: 20/40M
Data Rate (Mbps): 6 Mbps ☑ Auto
Transmit Power: 17 dBm
Rate Aggressiveness: 0
Channel Scan List: □ Enabled

Fig 2.4 Basic Wireless Settings (Station/Station WDS)

This options below are only available in **Station, Station WDS** and **Repeater WDS** modes unless otherwise stated.

Wireless Mode: Station

Remote AP-ESSID

This is the Service Set Identifier used by station to seek and connect to the access point of same the SSID identifier.

Site Survey

Site Survey will search for the available wireless networks in range on all the supported channels and will allowyou to select one for association. In case the selected network uses encryption, you ll need to set security parameters in wireless security section. Click Scan to re-scan the Access Points in range. Select the Access Point from the list and click Close this window. Site Survey channel scan list can be modified using the Channel Scan List control.

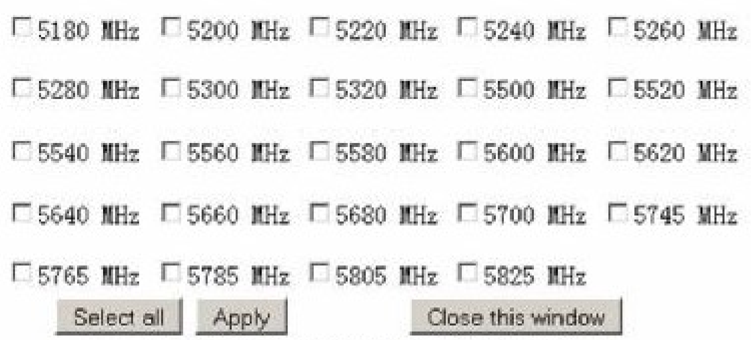
Remote AP Lock to MAC

Enter the MAC address of the remote access point the device is connected to. This option will make device only connect to this access point. This is important when connection is Point-to-Point operation.

Remote AP - Preferred MAC

Enter the preferred MAC address of the access point you want device to connect when it first startup. Up to max of 4 MAC addresses can be entered. Priority is fromtop to bottom. In the event all preferred MAC addresses are not available, device will then pick the matching SSID access point with the strongest signal.

Channel Scan List



□ 5180 MHz □ 5200 MHz □ 5220 MHz □ 5240 MHz □ 5260 MHz

□ 5280 MHz □ 5300 MHz □ 5320 MHz □ 5500 MHz □ 5520 MHz

□ 5540 MHz □ 5560 MHz □ 5580 MHz □ 5600 MHz □ 5620 MHz

□ 5640 MHz □ 5660 MHz □ 5680 MHz □ 5700 MHz □ 5745 MHz

□ 5765 MHz □ 5785 MHz □ 5805 MHz □ 5825 MHz

Fig 2.5 Channel Scan List (In US Country Code)

According to the availability of channels in the country codes, the operator can select which channels to be scanned when scanning for an Access Point. Then the scanned channels will appear on the Site Survey.

Wireless Adapter mode

This option change device function like a wireless adapter installed in a computer.

This mode should only be use on one computer, like old laptops or computer aided device with only Ethernet port like printer that do not have expansion interface to add wireless interface.

It work transparently forwarding and receiving packets fromwireless to the computer s ethernet port. The Ethernet port MACaddress of the client computer is cloned and copied on top of this device, so the opposite connecting device will register this MAC address of the laptop or PC rather than the intermediate wireless device. This option is effective for only one computer connection. If the computer device like printer that have not option to do the setup, it should first be configured froma PC then connect to the printer.

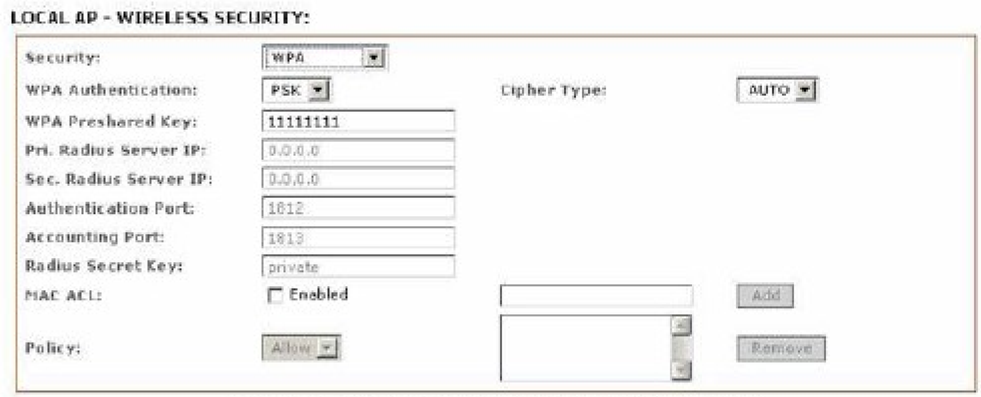
The configuration parameters are the same as Station mode as shown above.

4.3.4 Wireless Security

All the wireless security settings are set under this section.

The operation of the Keys is the same for ALL theWireless modes.

WPA or WPA2 Authentication



LOCAL AP - WIRELESS SECURITY:

Security: WPA

WPA Authentication: PSK

Cipher Type: AUTO

WPA Preshared Key: 11111111

Pri. Radius Server IP: 0.0.0.0

Sec. Radius Server IP: 0.0.0.0

Authentication Port: 1812

Accounting Port: 1813

Radius Secret Key: private

MAC ACL: □ Enabled

Policy: Allow

Fig 2.7 WPA (Access Point/Access Point WDS/Repeater WDS)

WPA PSK

PSK (Default) WPA or WPA2 with Pre-shared Key method.

Cipher Type

TKIP - Temporal Key Integrity Protocol which uses RC4 encryption algorithm.

AES - Advanced Encryption Standard (AES) algorithm.

AUTO(Default) Automatically select between both algorithms.

Preshared Key

This option is available when **WPA** or **WPA2**, with **PSK** selected.

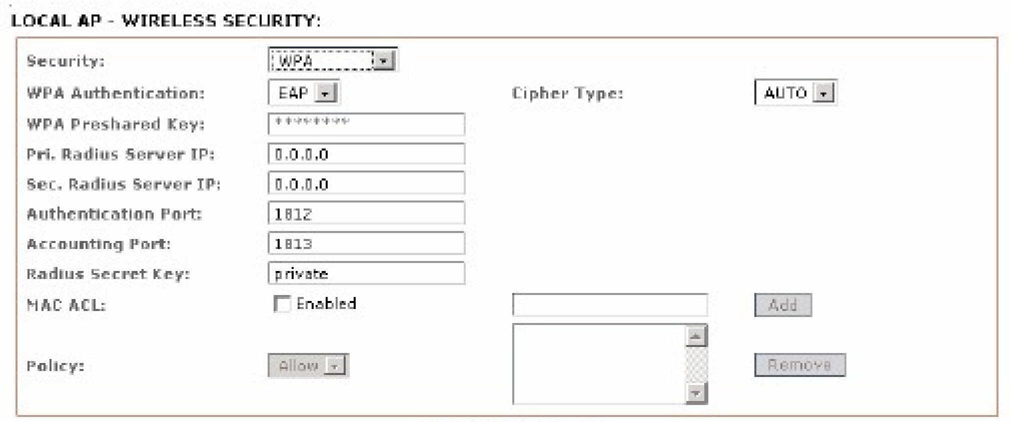
The pre-shared key is an alpha-numeric password between 8 and 63 characters long.

***** Important:**

802.11n network using WPA authentication should use AES cipher type for connection to ensure the highest transmission speed and throughput is switch on. Using TKIP cipher type device may switch to legacy maximumtransmission speed of 54Mbps. And performance can only achieve up to legacy maximum

performance and throughput.

WPA + EAP



LOCAL AP - WIRELESS SECURITY:

Security:	WPA		
WPA Authentication:	EAP	Cipher Type:	AUTO
WPA Preshared Key:	********		
Pri. Radius Server IP:	0.0.0.0		
Sec. Radius Server IP:	0.0.0.0		
Authentication Port:	1812		
Accounting Port:	1813		
Radius Secret Key:	private		
MAC ACL:	□ Enabled		Add
Policy:	Allow		Remove

Fig 2.8 WPA + EAP

EAP WPA orWPA2 with EAP (Extensible Authentication Protocol)

Firmware supported options for clients are: EAP-TLS, EAP-TTLS, PEAP

Cipher Type

TKIP - Temporal Key Integrity Protocol which uses RC4 encryption algorithm.

AES - Advanced Encryption Standard (AES) algorithm.

AUTO (Default) Automatically select between both algorithms.

Primary Radius Server IP

Enter the Primary Radius Server IP address .

Secondary Radius Server IP

Enter the Secondary Radius Server IP address .

Authentication Port

Enter the Authentication Port number of the Radius Server. Default is 1812.

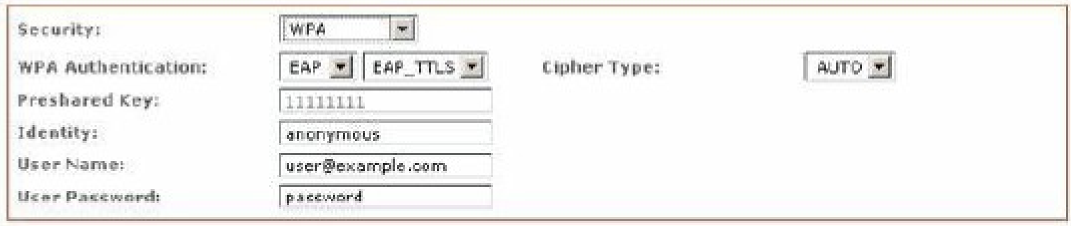
Accounting Port

Enter the Accounting Port number of the Radius Server. Default is 1813.

Radius Secret Key

Enter the Secret Key of the Radius Server. The device use this to authenticate itself into the Radius Server.

WPA + EAP_TLS, WPA-TTLS, WPA-PEAP



Security: WPA

WPA Authentication: EAP EAP_TTLS

Cipher Type: AUTO

Preshared Key: 11111111

Identity: anonymous

User Name: user@example.com

User Password: password

Fig 2.8WPA (Station /Station WDS/Repeater WDS)

This apply to the following modes only, when **WPA** or **WPA2**, with **EAP** is selected. **Station, Station WDS, Repeater WDS** mode.

Identity

Identification credential used by the wpa-supplicant for EAP authentication.

User Name:

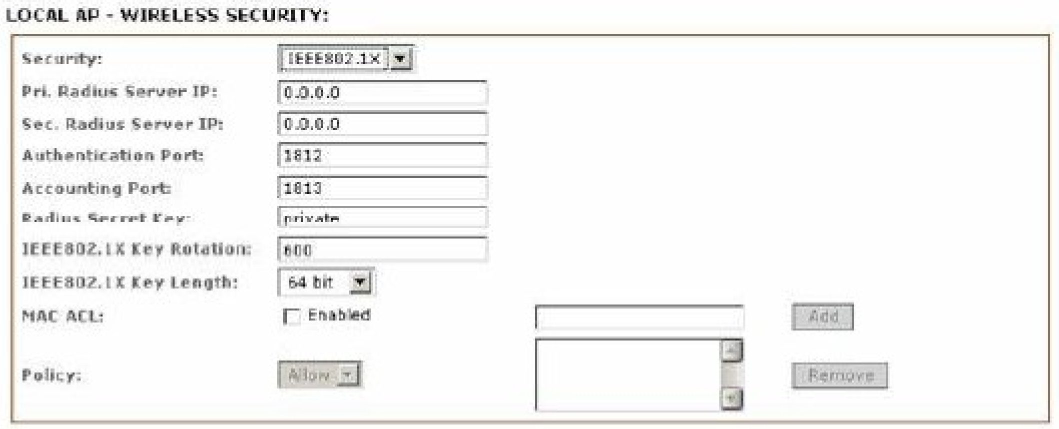
Identification credential used by the wpa-supplicant for EAP tunneled authentication in unencrypted form.

User Password:

Password credential used by the wpa-supplicant for EAP authentication

IEEE802.1x Settings

The operation of the Keys is the same for ALL the modes.



LOCAL AP - WIRELESS SECURITY:

Security:	IEEE802.1X
Pri. Radius Server IP:	0.0.0.0
Sec. Radius Server IP:	0.0.0.0
Authentication Port:	1812
Accounting Port:	1813
Radius Secret Key:	private
IEEE802.1X Key Rotation:	600
IEEE802.1X Key Length:	64 bit
MAC ACL:	□ Enabled
Policy:	Allow

Fig. 2.8 IEEE802.1X (Access Point/Access Point WDS/ Repeater WDS)

This option apply to the following modes only, when WPA EAP or IEEE802.1x .

Access Point, Access Point WDS, Repeater WDS modes.

Primary Radius Server IP

Enter the Primary Radius Server IP that Access Point will use to query server.

Secondary Radius Server IP

Enter the Secondary Radius Server IP that Access Point will use to query the server.

Authentication Port

Enter the Radius Server Authentication Port number to use. Default is 1812.

Accounting Port

Rnter Radius server Accounting Port to use. Default is 1813.

Radius Secret Key

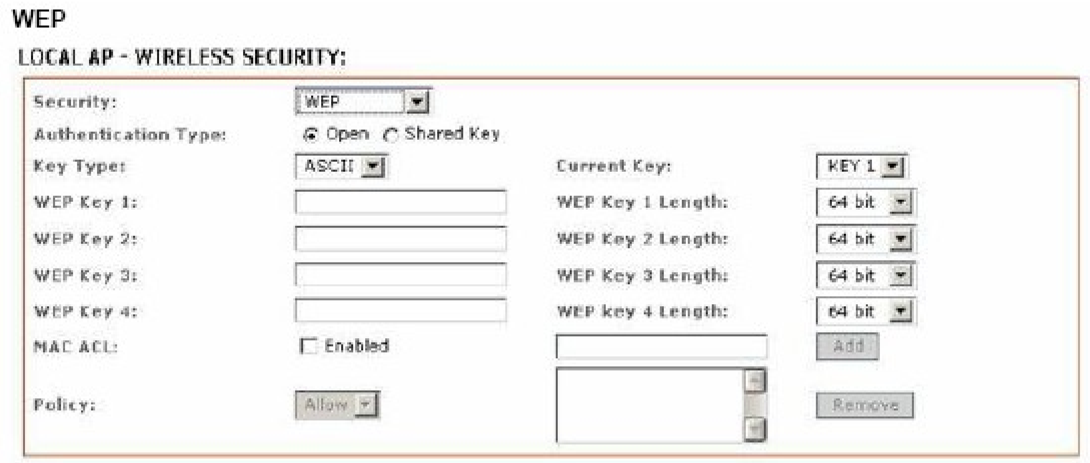
Enter Radius server Secret Key that Access Point to use to authenticate itself with radius server.

IEEE802.1x Key Rotation

Enter time in seconds. After time expired will initiate key rotation in uthentication process for higher security.

IEEE802.1x Key Length

This is the key length of the initial seed key. Select 64 or 128bit.



WEP

LOCAL AP - WIRELESS SECURITY:

Security:	WEP		
Authentication Type:	● Open ○ Shared Key		
Key Type:	ASCII	Current Key:	KEY 1
WEP Key 1:		WEP Key 1 Length:	64 bit
WEP Key 2:		WEP Key 2 Length:	64 bit
WEP Key 3:		WEP Key 3 Length:	64 bit
WEP Key 4:		WEP key 4 Length:	64 bit
MAC ACL:	□ Enabled		Add
Policy:	Allow		Remove

Fig 2.6 WEP

The operation of the Keys is the same for ALL the modes.

**** Note: Operating with WEP security will lower the performance significantly with 802.11n radio. Not recommended for Access Point and Access Point WDS mode operation. May use WEP ONLY when connecting with standard 11 and 54Mbps (legacy) 802.11a/b/g bands radio.**

Authentication Type:

Open Authentication (Default) No authentication. Recommend to use this standard option over shared authentication.

Shared Authentication May not be compatible with all Access Point. Not recommended.

Key Type:

HEX or **ASCII** option specifies the character format for the WEP key if WEP security method is used.

Current Key:

Specify the Index of theWEP Key used. 4 differentWEP keys can be configured at the same time, but only one is used.

WEP Key:

WEP encryption key for the wireless traffic encryption and decryption should be specified if WEP security method is used.

WEP Key Length:

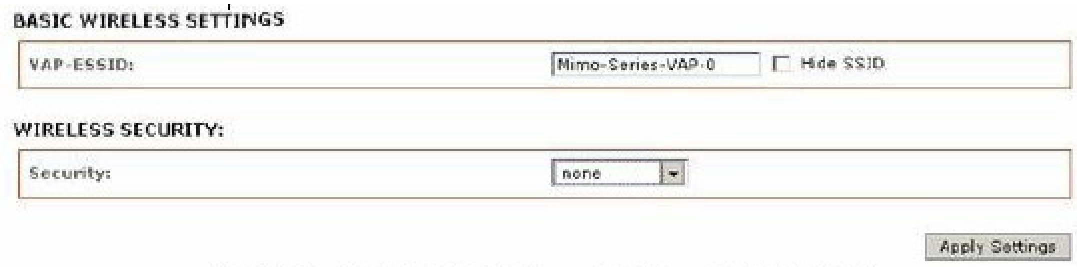
64-bit (selected by default) or 128-bitWEP Key length should be selected if WEP security method is used. The 128-bit option will provide higher level of security.

For **64-bi**t specifyWEP key as 5 HEX (0-9, A-F or a-f) pairs (e.g. 00112233AA) or 5 ASCII characters.

For **128-bit** specifyWEP key as 13 HEX (0-9, A-F or a-f) pairs (e.g. 00112233445566778899AABBCC) or 13 ASCII characters.

4.3.5 Virtual Access Point (VAP)

Virtual AP (VAP) implementsmSSID (Multi-SSID) whereby a single wireless card can be setup with up to 3 virtual SSID of BSSID connections. Each VAP can be set with different security authentication mode.



BASIC WIRELESS SETTINGS

VAP-ESSID: Mimo-Series-VAP-0 □ Hide SSID

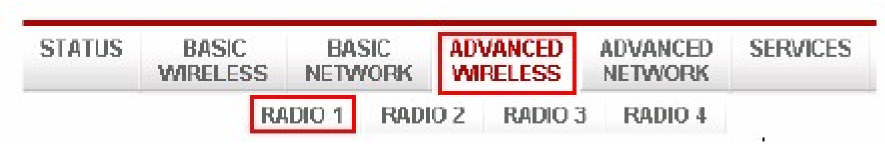
WIRELESS SECURITY:

Security: none

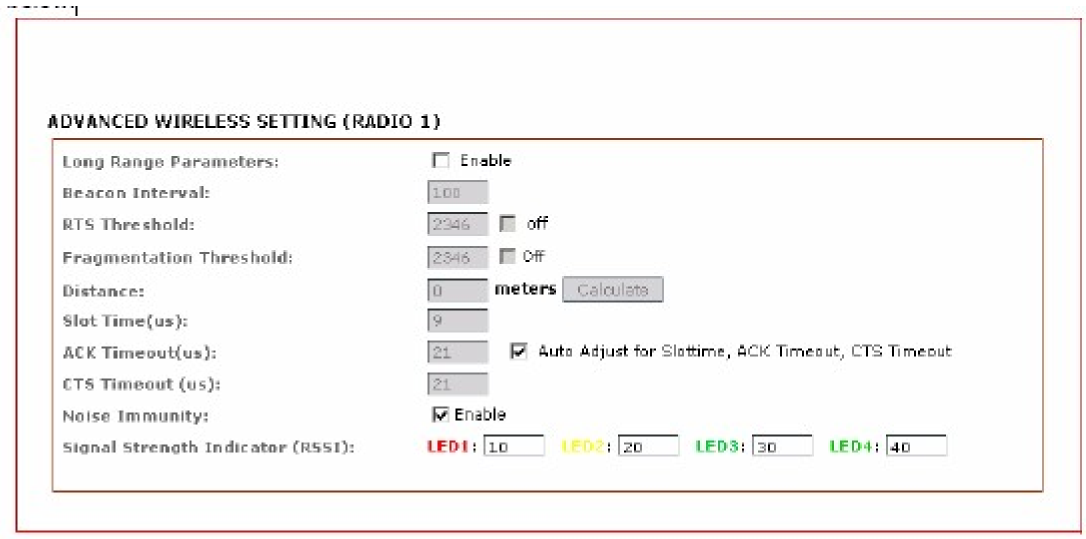
Fig 2.11 Virtual AP (Only Available in Access Point/ Access Point WDS Mode)

All VAPs are created fromthe same radio they all share the same wireless channel, country code, channel spectrumwidth and transmit power.

4.4 Advance Wireless Tab



Click **Advanced Wireless** tab frommenu and select **RADIO 1** to open the page below.



ADVANCED WIRELESS SETTING (RADIO 1)

Long Range Parameters: □ Enable

Beacon Interval: 100

RTS Threshold: 2346 □ off

Fragmentation Threshold: 2346 □ Off

Distance: 0 meters Calculate

Slot Time(us): 9

ACK Timeout(us): 21 ☑ Auto Adjust for Slottime, ACK Timeout, CTS Timeout

CTS Timeout (us): 21

Noise Immunity: ☑ Enable

Signal Strength Indicator (RSSI): LED1: 10 LED2: 20 LED3: 30 LED4: 40

4.4.1 Long Range Parameters Setup

Advanced wireless page let you setup outdoor long distant connection parameters.

Long Range Parameters:

Check to enable parameters.

Beacon Interval: (default is 100 ms)

Define the time interval (in millisecond) the beacon to broadcast.

Recommend to use default.

RTS Threshold: (Default is **OFF**)

Fragmentation Threshold: (Default is **OFF**)

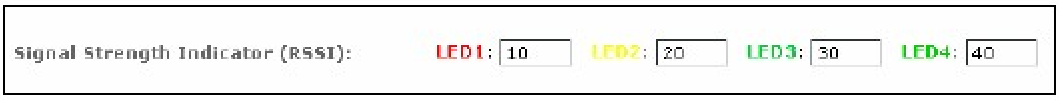
Distance:

Enter the distant in meters the device is to connect with the opposite device. Then click Calculate. The close approximate values for Slot Time, ACK Timeout, CTS Timeout will be calculated. Fine tuning can be further adjusted for the best environment conditions to achieve best performance and better link reliability.

Noise Immunity:

Check to enable. When enabled, it automatically adjusts the signal/noise level for best performance. In low noise environment it is recommended to turn off this function.

Signal Strength Indicator (RSSI):



Signal Strength Indicator (RSSI): LED1: 10 LED2: 20 LED3: 30 LED4: 40

The default values are LED1-Red (10), LED2-Yellow (20), LED3-Green (40)

Each LEDs when turn on indicates the RSSI signal strength has hit over the value.

e.g. When LED1 and LED2 light up it indicate the RSSI is greater than 20.

When all 4 LEDs light up it indicate RSSI is greater than 40.

For long distant installation when signal strength expected to be about 20-30, the values can be adjusted to display over this new range.

e.g. the LEDs values can be adjusted as follows:

LED1 (RSSI value=7)

LED2 (RSSI value=15)

LED3 (RSSI value=22)

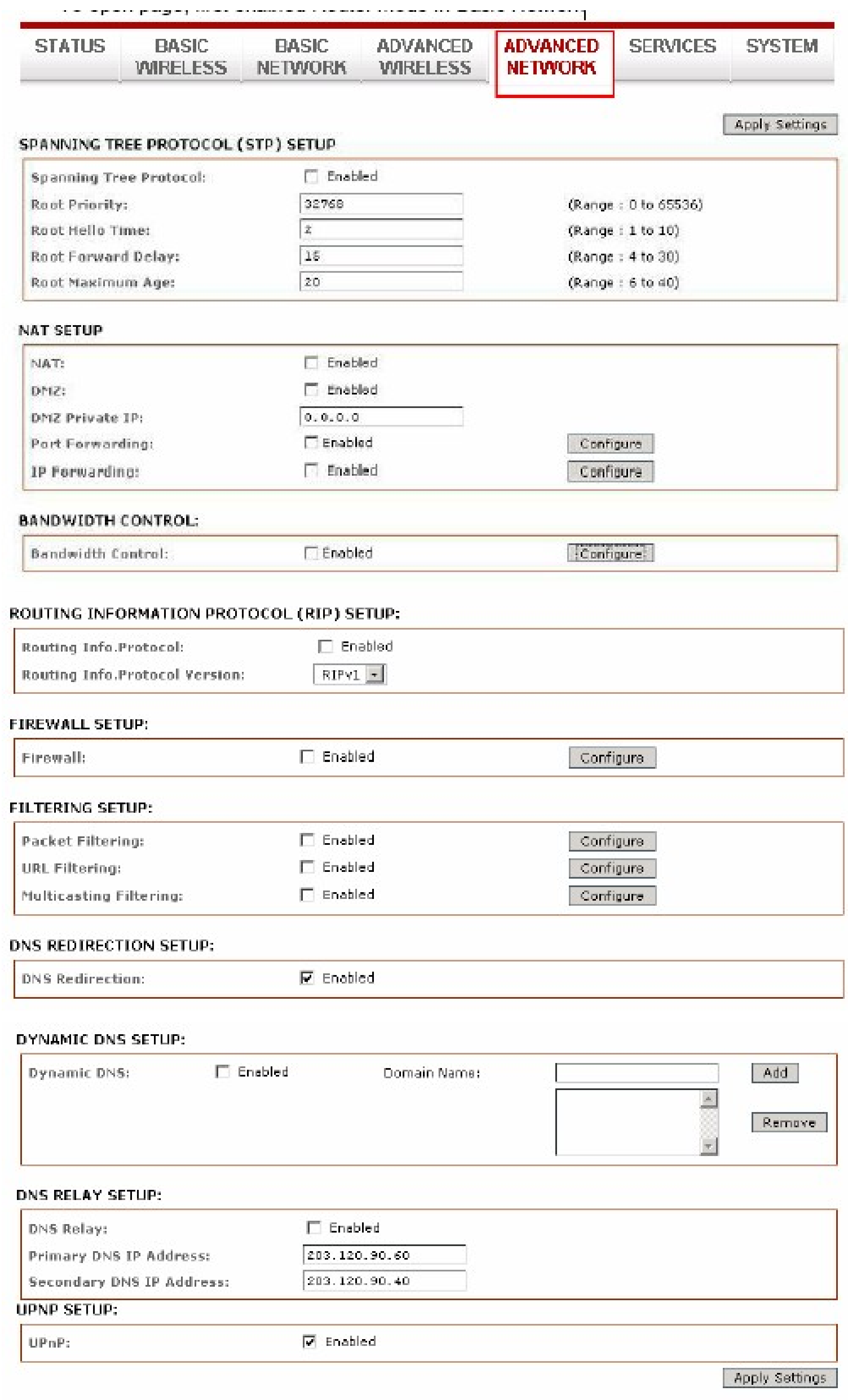
LED4 (RSSI value=27)

4.5 Advanced Network Tab

Click **Advanced Network** tab frommenu to open the page below.

***Note:** This tab will not open when in device is in Bridge node.

To open page, first enabled Router mode in Basic Network



SPANNING TREE PROTOCOL (STP) SETUP

Spanning Tree Protocol:	□ Enabled	
Root Priority:	32768	(Range : 0 to 65536)
Root Hello Time:	2	(Range : 1 to 10)
Root Forward Delay:	15	(Range : 4 to 30)
Root Maximum Age:	20	(Range : 6 to 40)

NAT SETUP

NAT:	□ Enabled	
DMZ:	□ Enabled	
DMZ Private IP:	0.0.0.0	
Port Forwarding:	□ Enabled	Configure
IP Forwarding:	□ Enabled	Configure

BANDWIDTH CONTROL:

Bandwidth Control:	□ Enabled	Configure

ROUTING INFORMATION PROTOCOL (RIP) SETUP:

Routing Info.Protocol:	□ Enabled
Routing Info.Protocol Version:	RIPv1

FIREWALL SETUP:

Firewall:	□ Enabled	Configure

FILTERING SETUP:

Packet Filtering:	□ Enabled	Configure
URL Filtering:	□ Enabled	Configure
Multicasting Filtering:	□ Enabled	Configure

DNS REDIRECTION SETUP:

DNS Redirection:	☑ Enabled

DYNAMIC DNS SETUP:

Dynamic DNS:	□ Enabled	Domain Name:		Add Remove

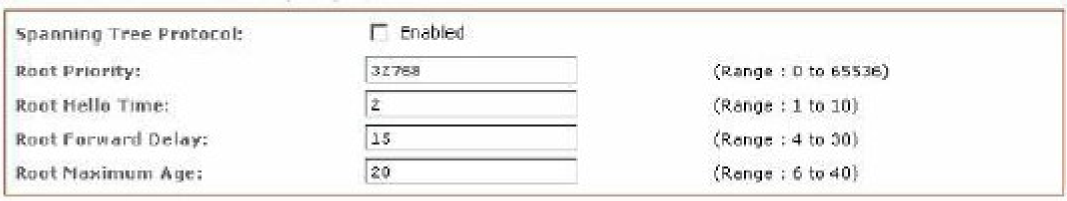
DNS RELAY SETUP:

DNS Relay:	□ Enabled
Primary DNS IP Address:	203.120.90.60
Secondary DNS IP Address:	203.120.90.40

UPNP SETUP:

UPnP:	☑ Enabled

4.5.1 Spanning Tree Setup



Spanning Tree Protocol:	□ Enabled	
Root Priority:	32768	(Range : 0 to 65536)
Root Hello Time:	2	(Range : 1 to 10)
Root Forward Delay:	15	(Range : 4 to 30)
Root Maximum Age:	20	(Range : 6 to 40)

Spanning Tree Protocol: Default is **disabled**. Check on box to enable.

Root Priority: Default value is 32768. Smaller value has higher priority.

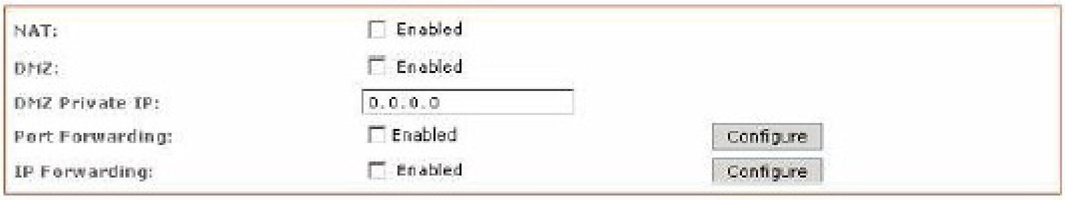
Root Hello Time: Default time is 2 seconds.

Root Forward Delay: Default is 15 seconds

Root MaximumAge: Default is 20 seconds

Changing to lower time can caused high overheads to the network.

4.5.2 NAT Setup



NAT:	□ Enabled	
DMZ:	□ Enabled	
DMZ Private IP:	0.0.0.0	
Port Forwarding:	□ Enabled	Configure
IP Forwarding:	□ Enabled	Configure

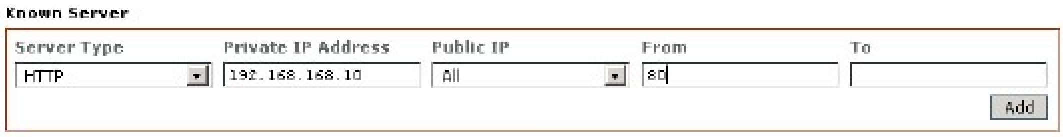
NAT: Enabled when in Router mode. Disabled when in Bridge mode.

DMZ: Default is disabled. Check on box to enable.

DMZ IP Address: Input IP address of the local PC to receive the DMZ packets.

Port Forwarding: Default is disabled. Check on box to enable.

For configuration refer to Appendix section.



Known Server

Server Type	Private IP Address	Public IP	From	To
HTTP	192.168.168.10	All	80	

Add

Adding an entry fromKnown Server

Add entry fromthis box and select an application the list.

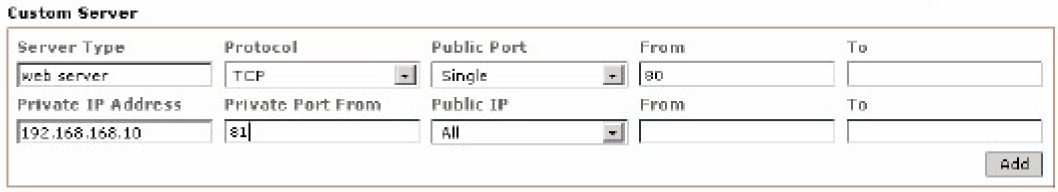
Server Type: click to select the application you want to add.

Private IP Address: Enter the local IP of the PC running the application

Public IP Address: If the application to for any people on the internet to access then select the default, **All**.

If only specific IP, select **Single** and enter the IP address.

If only specific range of IP, select **Range** and enter IP address range.



Custom Server

Server Type	Protocol	Public Port	From	To
web server	TCP	Single	80	
Private IP Address	**Private Port From**	**Public IP**	**From**	**To**
192.168.168.10	81	All		

Add

Adding an entry fromCustomServer

Entry from Custom Server box lets you enter the other port number service for an application and new applications.

Custom Server also lets you enter a different public and private port service

Server Type: Enter a brief name for the application. This info helps you track the application for that port number you set.

Protocol: Select TCP or UDP the application use.

Public Port: select Single or Range of ports application use.

From: if single port, enter this box only. If port range, enter starting port number here.

To: if single port, leave blank. if port range enter, enter last port number here.

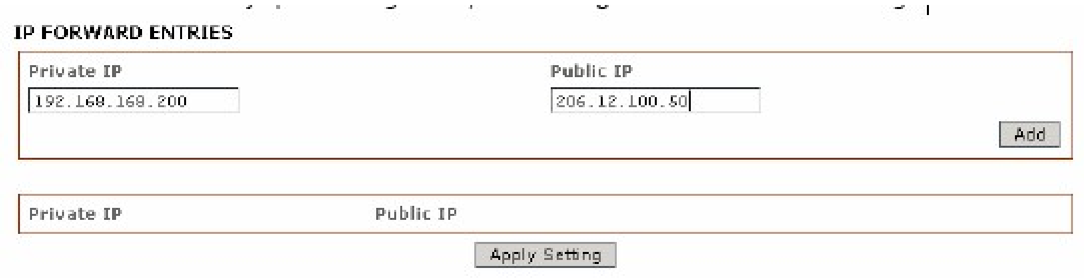
Private IP Address: Enter the local IP of the PC running the application

Private Port From: If single port, enter same public port number or new port number. If port range, enter only the starting port number.

Public IP Address: If the application is to access by any people on the internet, then select the default, **All**.

If only specific IP, select **Single** and enter the IP address.

If only specific range of IP, select **Range** and enter IP address range.



IP FORWARD ENTRIES

Private IP: 192.168.168.200

Public IP: 206.12.100.50

IP Forwarding: Default is disabled. Check on box to enable.

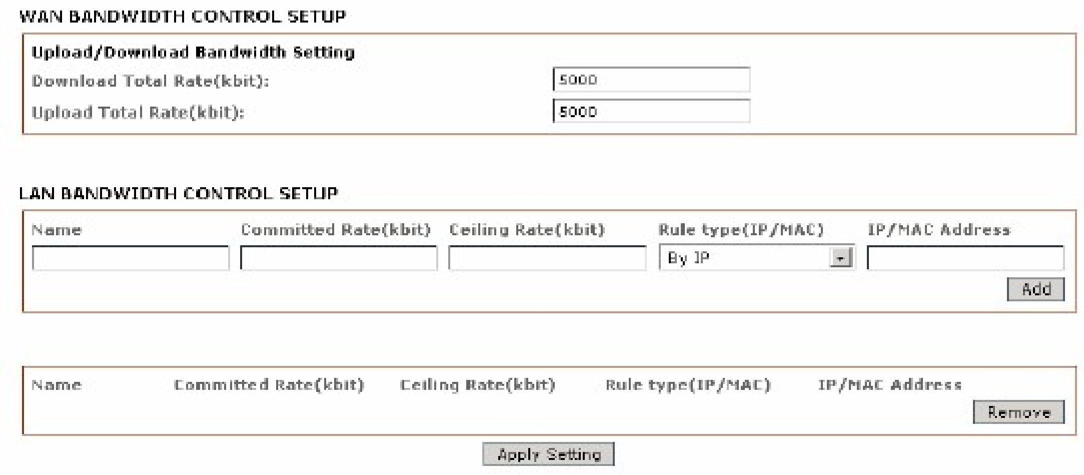
For configuration refer to Appendix section.

Private IP: enter the local IP address to receive forward packet by the public IP

Public IP: enter the public IP address when access will forward all packet to the local IP

Click Add to add to list.

4.5.3 Bandwidth Control



WAN BANDWIDTH CONTROL SETUP

Upload/Download Bandwidth Setting

Download Total Rate(kbit): 5000

Upload Total Rate(kbit): 5000

LAN BANDWIDTH CONTROL SETUP

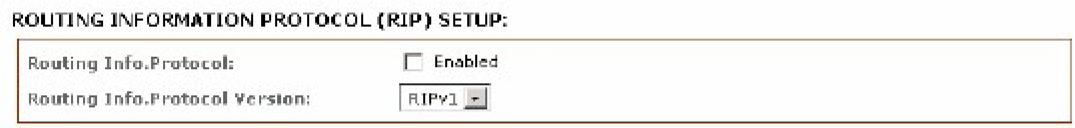
Rule type(IP/MAC): By IP

Bandwidth Control: Default is disabled. Check on box to enable.

This control let user set a max limited bandwidth to router.
This function let use share one high speed broadband line with several
routers each limited to a maximum limited by its bandwidth control.

Download Total Rate(kbit) enter the max bandwidth limit for downloading on this router.
Upload Total Rate(kbit): enter the max bandwidth limit for uploading on this router.

Upload/Download limit can also be controlled for each user by IP or MAC address.
Name: enter short name of user. Name track the user to rule only.
Committed Rate(kbit): enter the average rate for user.
Ceiling Rate (kbit): enter the peak rate allowed for user
Rule Type: select **By IP** or **By MAC**
IP/MAC Address: enter the local IP address if rule type is **By IP**
enter the local PC ethernet MAC address if rule type is **By MAC**

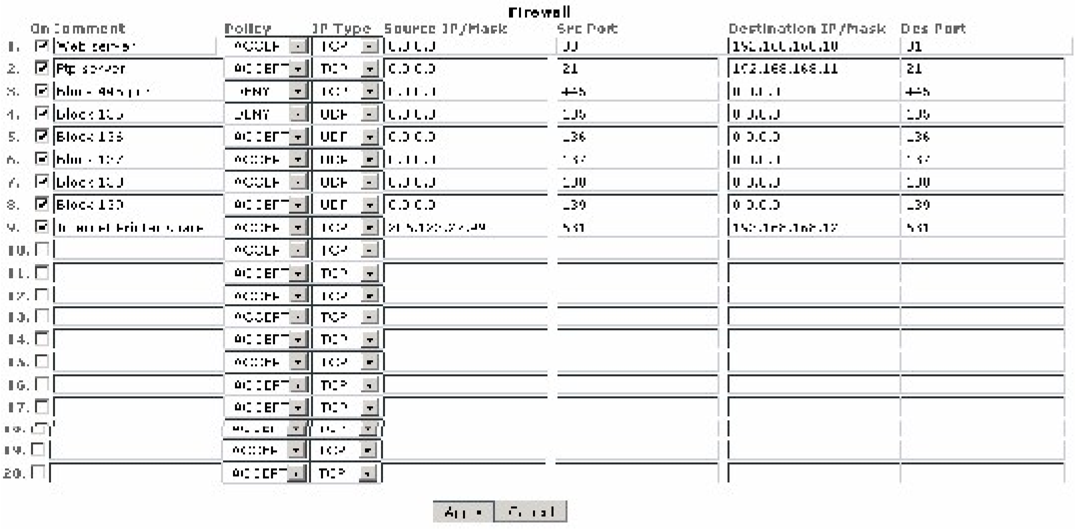


ROUTING INFORMATION PROTOCOL (RIP) SETUP:

Routing Info.Protocol:	□ Enabled
Routing Info.Protocol Version:	RIPv1

Routing Information Protocol: Default is disabled. Check on box to enable.
For configuration refer to Appendix section.
Router Info Protocol version: select RIPv1 or RIPv2

4.5.4 Firewall Setup



Firewall

	On	Comment	Policy	IP Type	Source IP/Mask	Src Port	Destination IP/Mask	Des Port
1.	☑	Web server	ACCEPT	TCP	0.0.0.0	80	192.168.168.10	81
2.	☑	Ftp server	ACCEPT	TCP	0.0.0.0	21	192.168.168.11	21
3.	☑	Block 445 port	DENY	TCP	0.0.0.0	445	0.0.0.0	445
4.	☑	Block 135	DENY	UDP	0.0.0.0	135	0.0.0.0	135
5.	☑	Block 136	ACCEPT	UDP	0.0.0.0	136	0.0.0.0	136
6.	☑	Block 137	ACCEPT	UDP	0.0.0.0	137	0.0.0.0	137
7.	☑	Block 138	ACCEPT	UDP	0.0.0.0	138	0.0.0.0	138
8.	☑	Block 139	ACCEPT	UDP	0.0.0.0	139	0.0.0.0	139
9.	☑	Internet Printer share	ACCEPT	TCP	[illegible]	[illegible]	192.168.168.12	[illegible]
10.	□		ACCEPT	TCP				
11.	□		ACCEPT	TCP				
12.	□		ACCEPT	TCP				
13.	□		ACCEPT	TCP				
14.	□		ACCEPT	TCP				
15.	□		ACCEPT	TCP				
16.	□		ACCEPT	TCP				
17.	□		ACCEPT	TCP				
18.	□		ACCEPT	TCP				
19.	□		ACCEPT	TCP				
20.	□		ACCEPT	TCP				

Firewall Setup: Default is disabled. Check on box to enable.
For configuration refer to Appendix section.
Comment: enter a brief name for the service.
Policy: select Accept or Deny for the apply rule
IP Type: select ICMP, TCP, and UDP packet type to check

Source IP/Mask: enter the source IP address and Netmask

Is the source IP of the packet (specified within the packet header), usually it is

the IP of the host system which sends the packets;

Src Port: enter the source port number in rule check

Is the source port of the TCP/UDP packet (specified within the packet header), usually it

is the port of the host system application which sends the packets.

Destination IP/Mask: enter the destination IP and Netmask

Is the Destination IP of the packet (specified within the packet header),

usually it is the IP of the system which the packet is addressed to;

Des Port: enter the destination port in rule check

Is the destination port of the TCP/UDP packet (specified within the packet

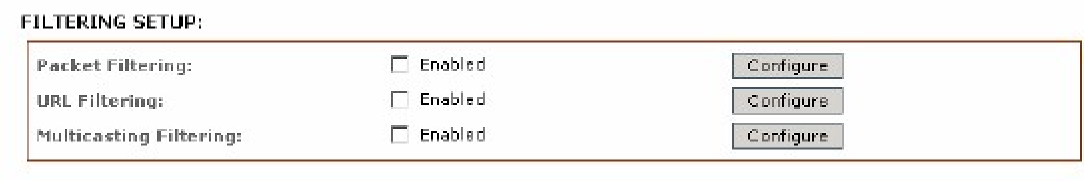
header), usually it is the port of the host system application which the packet is

addressed to

.

Click **Apply** to the rule or **Cancel** to clear the rule set.

Outbound Filtering Setup

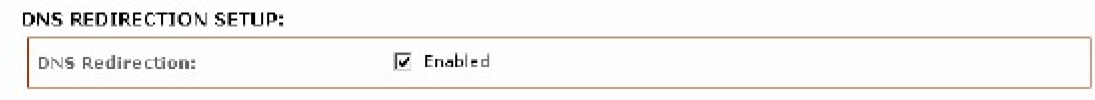


FILTERING SETUP:

Packet Filtering:	□ Enabled	Configure
URL Filtering:	□ Enabled	Configure
Multicasting Filtering:	□ Enabled	Configure

Filtering Setup: Default is disabled. Check on box to enable.

For configuration refer to Appendix section.



DNS REDIRECTION SETUP:

DNS Redirection: ☑ Enabled

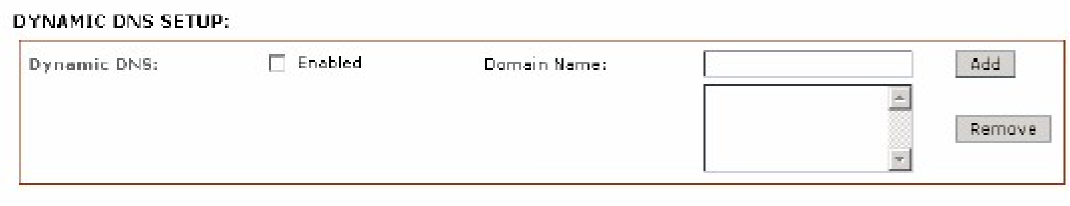
DNS Redirection: Default is enabled. Check on box to disable.

When enabled, router device will act as DNS proxy.

PC connected to this router device to set their TCPIP DNS IP to

router s IP address.

PC can still setup a valid DNS IP to skip the DNS proxy handling.



DYNAMIC DNS SETUP:

Dynamic DNS: □ Enabled Domain Name:

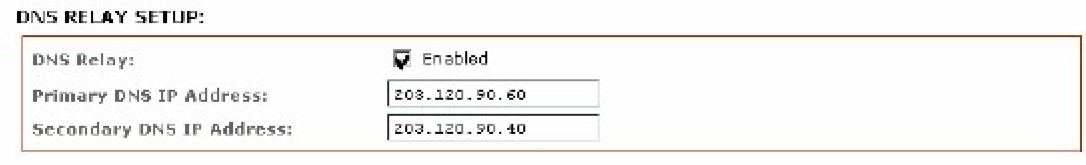
Dynamic DNS Setup: Default is disabled. Check on box to enable.

Dynamic DNS let router sWAN dynamic IP address linked and

automatically updated to domain server hosting the service each time the

IP address is changed. These ensured users on the internet can always get access to the hosting service behind the router.

For configuration refer to Appendix section.



DNS RELAY SETUP:

DNS Relay: ☑ Enabled

Primary DNS IP Address: 203.120.90.60

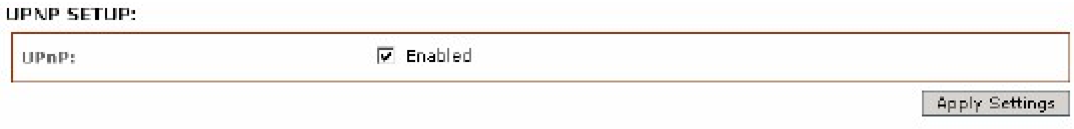
Secondary DNS IP Address: 203.120.90.40

DNS Relay Setup: Default is disabled. Check on box to enable.

These are the primary and secondary DNS IPs device proxy service use to resolve the domain name on behalf of the client PCs.

Primary DNS IP Address: Enter the primary DNS IP address

Secondary DNS IP Address: Enter the secondary DNS IP address



UPNP SETUP:

UPnP: ☑ Enabled

UPNP: Default is disabled. Check on box to enabled.

When enabled, client PC running Microsoft UPnP services can automatically open certain specific port required by the PC application in the router.

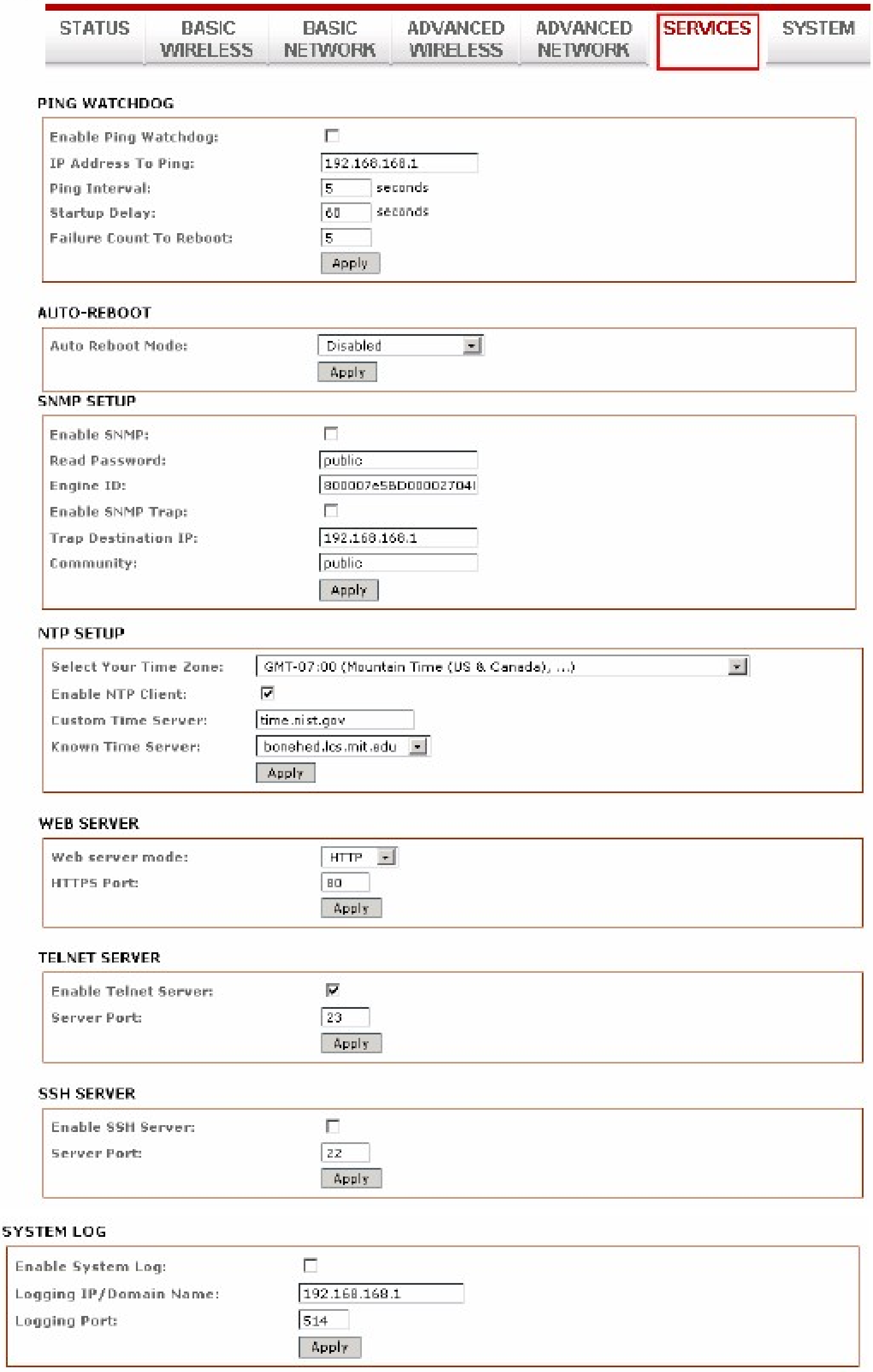
For security reason this service should not be open.

Recommend to setup manually open all port service through **Port Forwarding** service.

4.6 Services Tab

Click **Services** tab frommenu to open the page below.

Services section provides varieties of useful and enhanced functions to help assist device operations.



PING WATCHDOG

Enable Ping Watchdog:	□
IP Address To Ping:	192.168.168.1
Ping Interval:	5 seconds
Startup Delay:	60 seconds
Failure Count To Reboot:	5
	Apply

AUTO-REBOOT

Auto Reboot Mode:	Disabled
	Apply

SNMP SETUP

Enable SNMP:	□
Read Password:	public
Engine ID:	800007e5BD00002704
Enable SNMP Trap:	□
Trap Destination IP:	192.168.168.1
Community:	public
	Apply

NTP SETUP

Select Your Time Zone:	GMT-07:00 (Mountain Time (US & Canada), ...)
Enable NTP Client:	☑
Custom Time Server:	time.nist.gov
Known Time Server:	bonehed.lcs.mit.edu
	Apply

WEB SERVER

Web server mode:	HTTP
HTTPS Port:	80
	Apply

TELNET SERVER

Enable Telnet Server:	☑
Server Port:	23
	Apply

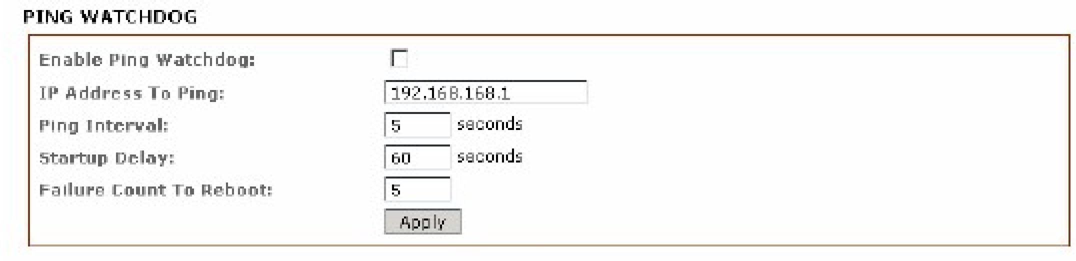
SSH SERVER

Enable SSH Server:	□
Server Port:	22
	Apply

SYSTEM LOG

Enable System Log:	□
Logging IP/Domain Name:	192.168.168.1
Logging Port:	514
	Apply

4.6.1 Ping Watchdog


PING WATCHDOG

Enable Ping Watchdog: □
IP Address To Ping: 192.168.168.1
Ping Interval: 5 seconds
Startup Delay: 60 seconds
Failure Count To Reboot: 5

Enable Ping Watchdog: Default is disabled. Check on box to enable.

IP Address To Ping: Target IP address do ping test monitor.

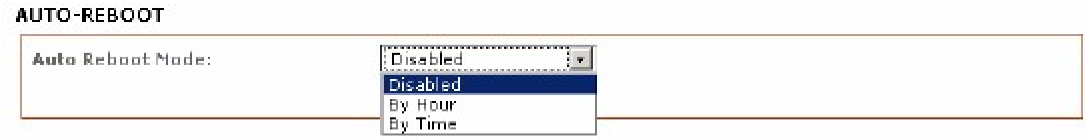
Ping Interval: Default is 5 seconds (minimum). This is Ping test duration.

Startup Delay: Default is 60 seconds(minimum).

One time delay after device startup.

Failed Count To Reboot: Default is 5. This is the number of ping failure count before device kick in the reboot process.

4.6.2 Auto-Reboot


AUTO-REBOOT

Auto Reboot Mode: Disabled

Auto-Reboot Mode: Default is disabled. Select By Hour or By Time check.

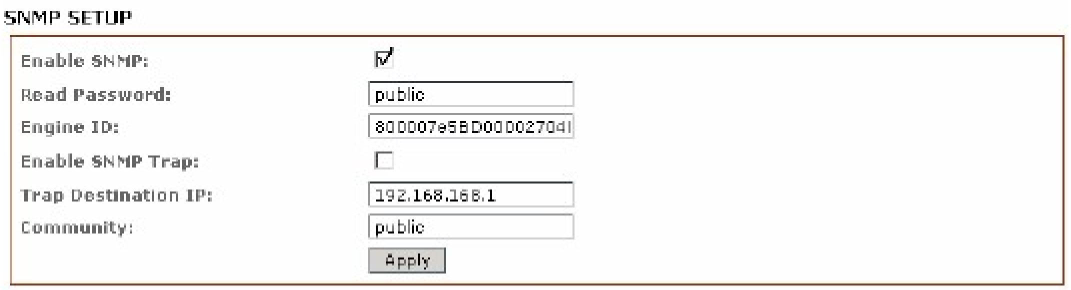
This mode lets you preset a timer to automatically force a reboot.

Timer can in fixed number of hours or at a specified time of day.

By Hour: Enter the number of hours device need to run before kick start reboot process.

By Time: Enter the specific time of day in hh:mm (24-hour format) to kick start reboots process.

4.6.3 SNMP Setup


SNMP SETUP

Enable SNMP: ☑
Read Password: public
Engine ID: 800007e5BD00002704I
Enable SNMP Trap: □
Trap Destination IP: 192.168.168.1
Community: public

Enable SNMP: Default is disabled. Check on box to enable.

Read Only Password: Password to query device.

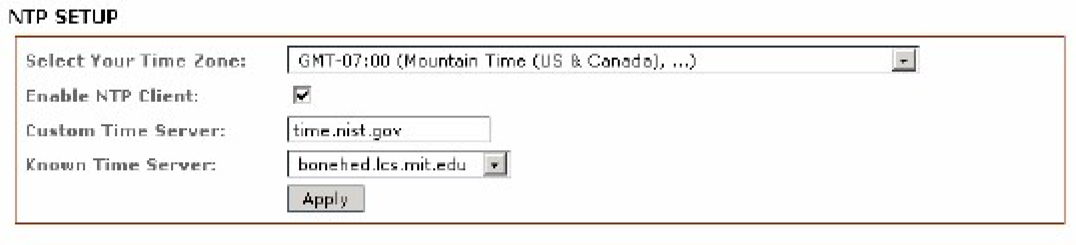
Engine ID: Default is 800007e5BD00002704D000007c

Enable SNMP Trap: Default is disabled. Check on box to enable.

Trap Destination IP: Enter the IP to send the info when trap is triggered.

Community: Enter the SNMP community string.

4.6.4 NTP Setup



NTP SETUP

Select Your Time Zone: GMT-07:00 (Mountain Time (US & Canada), ...)

Enable NTP Client: ☑

Custom Time Server: time.nist.gov

Known Time Server: bonehed.lcs.mit.edu

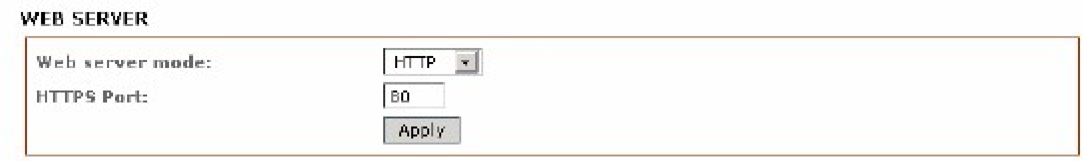
Select Your Time Zone: Select from list the country you reside.

Enable NTP Client: Default is disabled. Check on box to enable.

CustomTime Server: Default is time.nist.gov Enter preferred time server domain or IP

Known Time Server: You can also select one from this list as your new time server.

4.6.5 Web HTTP Security



WEB SERVER

Web server mode: HTTP

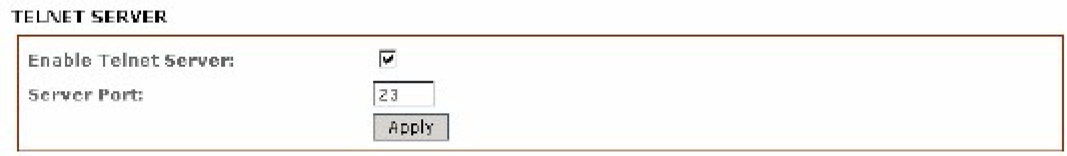
HTTPS Port: 80

Web Server Mode: Default is HTTP. Option is HTTP and HTTPs

HTTP(s) Port: Default is 80 for HTTP and 413 for HTTPs.

Enter a new preferred port number.

4.6.6 Telnet Access Setup



TELNET SERVER

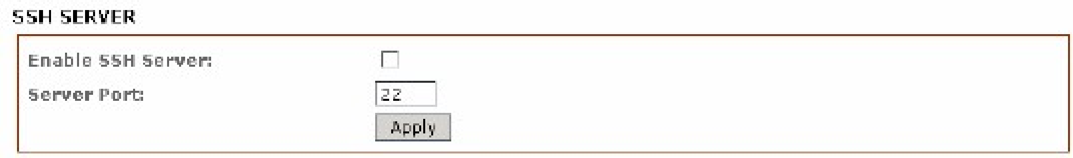
Enable Telnet Server: ☑

Server Port: 23

Enable Telnet Server: Default is enabled. Remove check on box to disable.

Server Port: Default is 23. Enter new preferred port number.

4.6.7 SSH Access Setup



SSH SERVER

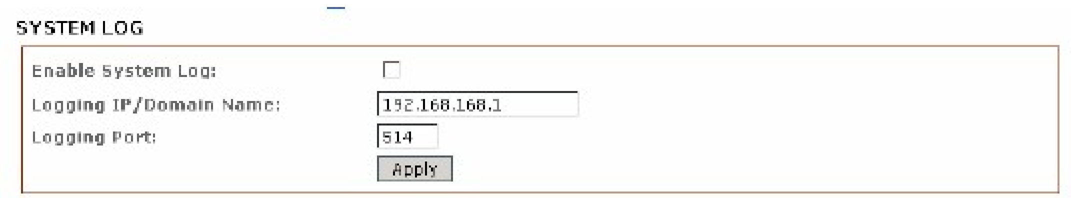
Enable SSH Server: □

Server Port: 22

Enable SSH Server: Default is disabled. Check on box to enable.

Server Port: Default is 22. Enter new preferred port number.

4.6.8 SystemLog Setup



SYSTEM LOG

Enable System Log: □

Logging IP/Domain Name: 192.168.168.1

Logging Port: 514

Enable SystemLogging: Default is disabled. Check on box to enable.

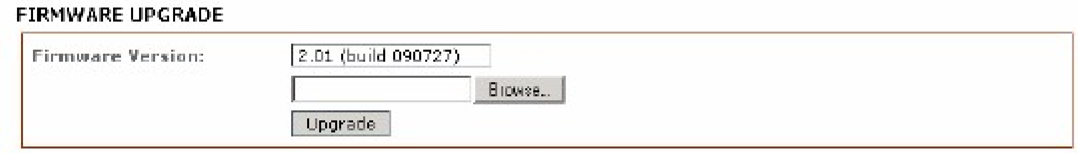
Logging IP /Domain Name: Enter destination IP address of device to receive log.

Logging Port: Default is 514. Enter the new preferred port number.

4.7 SystemTab

The System Page contains Administrative options. This page enables administrator to customize, reboot the device, set it to factory defaults, upload a new firmware, backup or update the configuration and configure administrator s credentials.

4.7.1 Firmware Upgrade



FIRMWARE UPGRADE

Firmware Version: 2.01 (build 090727)

Use this section to find out current software version and update the device with the new firmware. The device firmware update is compatible with all configuration settings. Systemconfigurations are preserved while the device is updated with a newfirmware version.

Firmware version: displays the version of the current firmware of the device system.

Upgrade: button opens the Firmware Upload window if activated.

Current Firmware: displays the version of the device firmware which is currently operating.

Firmware File: activate Browse button to navigate to and select the newfirmware file. The full path to the new firmware file location can be specified there. New firmware file is transferred to the system after Upload button is activated.

Close this window button cancels the new firmware upload process if activated.

Upgrade button should be activated in order to proceed with firmware upgrade routine (new irmware image should be uploaded into the system first). Please be patient, as the firmware upgrade routine can take 3-7 minutes. The based device will be un-accessible until the firmware upgrade routine is completed.

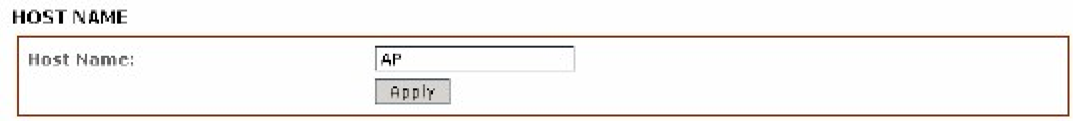
Do not switch off, do not reboot and do not disconnect the device fromthe power supply during the firmware upgrade process as these actions will damage the device!

It is highly recommended to backup the system configuration and the Support Info file before uploading the new configuration.

Close this window button closes the firmware upgrade window if activated.

This action will not cancel the firmware upgrade process.

4.7.2 Host Name



HOST NAME

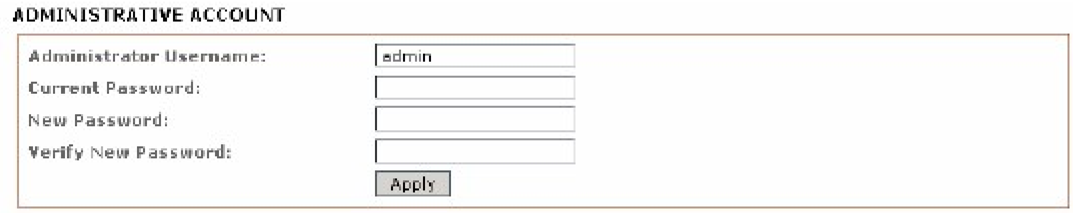
Host Name: AP

Host Name is the system wide device identifier. It is reported by SNMP Agent to authorized management stations. Host Name will be represented in popular Router Operating Systems registration screens and discovery tools.

Host Name: specifies the system identity.

Change button saves the Host Name if activated.

4.7.3 Administrative and Read-only Account



ADMINISTRATIVE ACCOUNT

Administrator Username: admin

Current Password:

New Password:

Verify New Password:

In this section you can modify the administrator password to protect your device from unauthorized configuration. The default administrator s password should be changed on the very first systemsetup:

Administrator Username: specifies the name of the system user.

Current Password: administrator is required to enter a current password. It is required for Password or Administrator Username change routine.

Default administrator login credentials:

User Name: **admin**

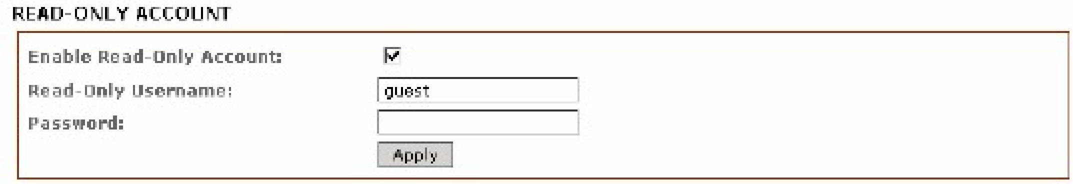
Password: **password**

New Password: new password used for administrator authentication should be specified.

Verify Password: new password should be re-entered to verify its accuracy.

Click Change button to save the changes.

4.7.4 Enable Read-Only Account



READ-ONLY ACCOUNT

Enable Read-Only Account: ☑

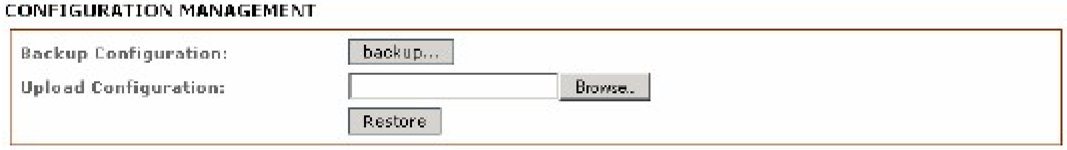
Read-Only Username: guest

Password:

Read-Only Username

Password: new password used for read-only administrator authentication should be specified.

4.7.5 Configuration Management



CONFIGURATION MANAGEMENT

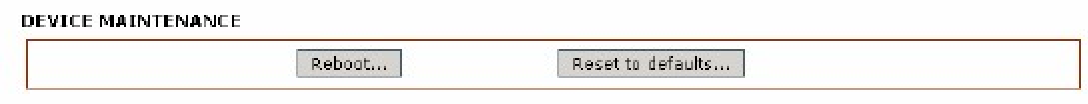
Backup Configuration:

Upload Configuration:

Backup Configuration: click Download button to export the current configuration to a file.

Upload Configuration: click Browse button to navigate to and select the new configuration file or specify the full path to the configuration file location.
Activating the Upload button will transfer new configuration file to the system.
New configuration will be effective after the Apply button is activated and systemreboot cycle is completed. Previous systemconfiguration is deleted after Apply button is activated. It is highly recommended to backup the systemconfiguration before uploading the new configuration.
Use only configuration backups of the same type device - configuration backed up from PowerStation2 suits only PowerStation2, but not LiteStation2 or LiteStation5! Behavior may be unpredictable when mixing configurations from different type devices.

4.7.6 Device Maintenance



DEVICE MAINTENANCE

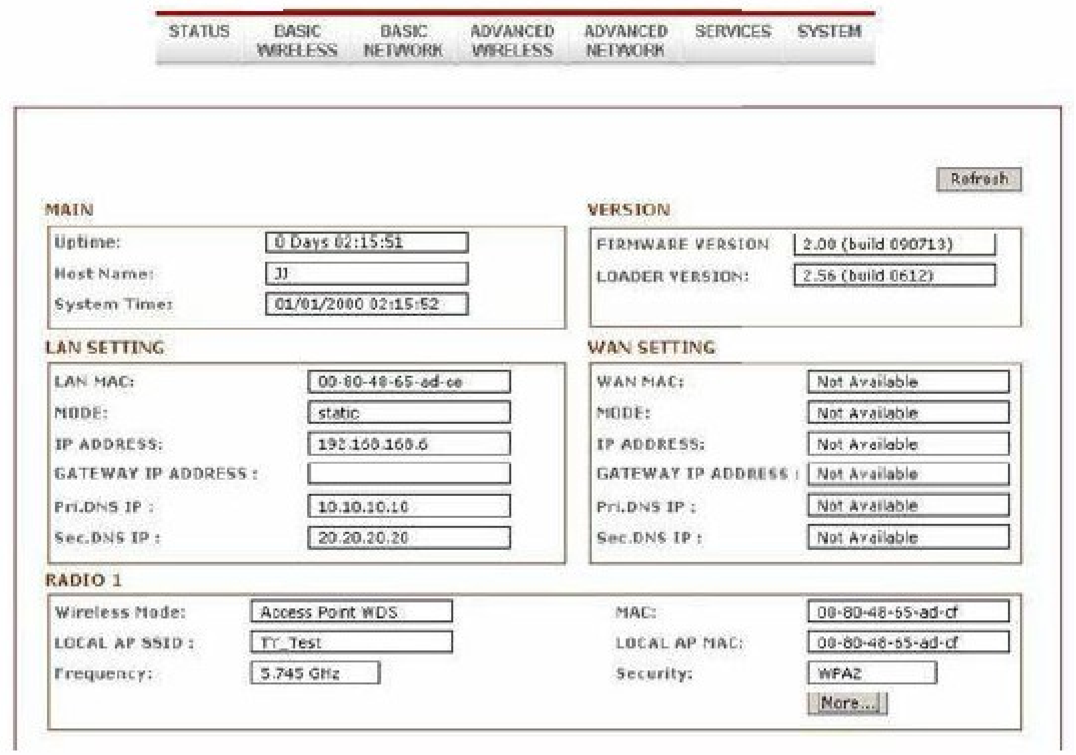
The controls in this section are dedicated for the device maintenance routines: rebooting, resetting, generating of the support information report.

Reboot: activate Reboot control in order to initiate full reboot cycle of the device. Reboot effect is the same as the hardware reboot which is similar to the power off - power on cycle. The system configuration is not modified after the reboot cycle completes. Any non-applied changes will be lost.

Reset to Defaults: activate Reset to Defaults control in order to initiate reset the device to factory defaults routine. Reset routine initiates system Reboot process (similar to the power off - power on cycle). The running systemconfiguration will be deleted and the default systemconfiguration (all the system settings with no exception) will be set.

After the **Reset to Defaults** routine is completed, the device systemwill return to the default IP configuration (192.168.168.1/255.255.255.0) and will start operating in Station-Bridge mode. It is highly recommended to backup the systemconfiguration before the Reset to Defaults is initiated.

4.8 Status Page



MAIN

Uptime:	0 Days 02:15:51
Host Name:	JJ
System Time:	01/01/2000 02:15:52

VERSION

FIRMWARE VERSION	2.00 (build 090713)
LOADER VERSION:	2.56 (build 0612)

LAN SETTING

LAN MAC:	00-80-48-65-ad-ce
MODE:	static
IP ADDRESS:	192.168.168.6
GATEWAY IP ADDRESS :	
Pri.DNS IP :	10.10.10.10
Sec.DNS IP :	20.20.20.20

WAN SETTING

WAN MAC:	Not Available
MODE:	Not Available
IP ADDRESS:	Not Available
GATEWAY IP ADDRESS :	Not Available
Pri.DNS IP :	Not Available
Sec.DNS IP :	Not Available

RADIO 1

Wireless Mode:	Access Point WDS	MAC:	00-80-48-65-ad-cf
LOCAL AP SSID :	TY_Test	LOCAL AP MAC:	00-80-48-65-ad-cf
Frequency:	5.745 GHz	Security:	WPA2

The Status Page displays a summary of link status information, current values of basic configuration settings (depending on operating mode), network settings and traffic statistics of all the interfaces.

4.8.1 Status Reporting

Main

Uptime: displays device up time since boot up. The time is expressed in days, hours, minutes and seconds.

Host Name: displays the assigned device host name (ID).

SystemTime: display device current date and time. Accurate system date and time is retrieved fromthe internet services using NTP (Network Time Protocol) if device is setup and connected to internet. Otherwise, the date and time update from device own inaccurate autonomous clock.

Version Firmware Version: displays current firmware version in operation.

Loader Version: displays current loader version of the device.

4.8.2 LAN Setting

LAN MAC: displays the MAC address of the device LAN (Ethernet) interface.

LAN Mode: displays the mode used, either static or DHCP client.

LAN IP Address: displays the current IP address of the LAN (Ethernet) interface.

LAN Gateway IP Address: displays the IP address of the gateway used in LAN.

LAN Pri. DNS IP: displays the Primary DNS IP address of the LAN setting.

LAN Sec. DNS IP: displays the Secondary DNS IP address of the LAN setting.

WAN Setting

WAN MAC: displays the MAC address of the deviceWAN interface.

WAN Mode: displays the mode used, either DHCP, PPPoE or Static IP.

WAN IP Address: displays the current IP address of theWAN interface.

WAN Gateway IP Address: displays the IP address of the gateway used inWAN.

WAN Pri. DNS IP: displays the Primary DNS IP address of the WAN setting.

WAN Sec. DNS IP: displays the Secondary DNS IP address of theWAN setting.

Radio

Wireless Mode: displays the current operating mode of the device.

Local AP SSID: displays the current SSID (Service Set Identifier) of device when operates in access point mode.

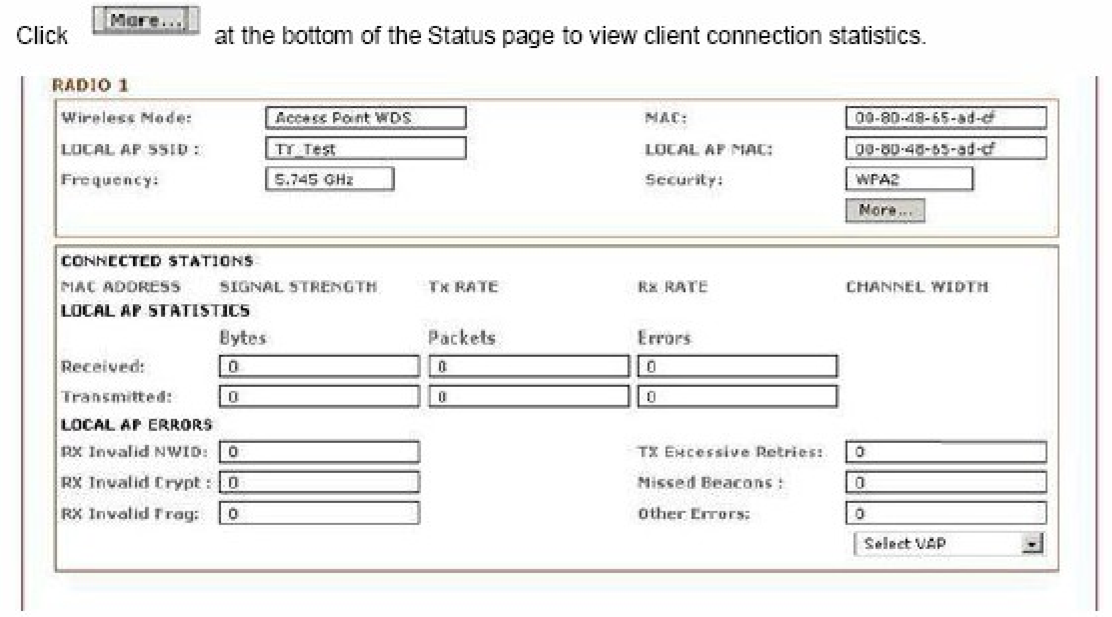
Frequency: displays current operating frequency running in device.

WLAN MAC: displays the MAC address or BSSID of the current activeWLAN card running in device.

WLAN Local/Remote AP MAC: displays the MAC address of theWLAN card connected to it.

WLAN Security: display the current active security mode.

4.8.3 Station Connection Status Info



Click More... at the bottom of the Status page to view client connection statistics.

RADIO 1

Wireless Mode: Access Point WDS
LOCAL AP SSID : TT_Test
Frequency: 5.745 GHz
MAC: 00-80-48-65-ad-cf
LOCAL AP MAC: 00-80-48-65-ad-cf
Security: WPA2

CONNECTED STATIONS

MAC ADDRESS	SIGNAL STRENGTH	Tx RATE	Rx RATE	CHANNEL WIDTH

LOCAL AP STATISTICS

	Bytes	Packets	Errors
Received:	0	0	0
Transmitted:	0	0	0

LOCAL AP ERRORS

RX Invalid NWID:	0	TX Excessive Retries:	0
RX Invalid Crypt :	0	Missed Beacons :	0
RX Invalid Frag:	0	Other Errors:	0

WLAN Connected Status:

MAC Address: displays the MAC address of the current activeWLAN card.

Signal Strength: displays the received wireless signal level of opposite connected device.

TX Rate and RX Rate: displays the current 802.11 data transmission (TX) and data reception (RX) rate while operating in Station mode. Typically, the higher the signal, the higher the data rate and consequently the higher the data throughput.

Channel Width:

20MHz is the standard channel spectrum width (selected by default).

40MHz the widest channel spectrum width required to connect to an 802.11a network which supports Static Turbo feature

WLAN Local AP Statistics:

Bytes transmitted/received value represents the total amount of data (in bytes) transmitted and received during the connection;

WLAN Local AP Errors: section displays the counters of 802.11 specific errors which were registered on wireless interface:

Rx invalid NWID value represents the number of packets received with a different NWIDor ESSID - packets which were destined for another access point. It can help to detect configuration problems or identify the adjacent wireless network existence on the same frequency.

Rx Invalid Crypt value represents the number of transmitted and received packets which were encrypted with the wrong encryption key and failed the decryption routines. It can be used to detect invalid wireless security settings and encryption break attempts.

Rx Invalid Frag value represents the number of packets missed during transmission and reception. These packets were dropped due to re-assembling failure as some link layer fragments of the packet were lost.

Tx Excessive Retries value represents the number of packets which failed to be delivered to the destination. Undelivered packet are retransmitted a number of times before an error occurs.

Missed beacons value represents the number beacons (management packets sent at regular intervals by the Access Point) which were missed by the client. This can indicate that the wireless client is out of range.

Other errors value represents the total number of transmitted and received packets that were lost or discarded for other reasons.

Appendix I - Network

This section provides more detailed explanation on the network operation modes in general.

The Network Page allows the administrator to setup bridge or routing functionality.

Device can operate in bridge or router mode. The IP configuration as described below is required for device management purposes. IP addresses can either be retrieved froma DHCP server or configured manually. Use the Network menu to configure the IP settings.

Network Mode Selections

Network Mode: Specify the operating network mode for the device.

The mode depends on the network topology requirements:

Bridge operating mode is selected by default as it is widely used by the subscriber stations, while connecting to Access Point or usingWDS. In this mode the device will act as a transparent bridge and will operate in Layer 2. There will be no network segmentation while broadcast domain will be the same. Bridge mode will not block any broadcast or multicast traffic. Additional Firewall settings can be configured for Layer 2 packet filtering and access control in

Bridge mode.

Router operating mode can be configured in order to operate in Layer 3 to perform routing and enable network segmentation wireless clients will be on different IP subnet.

Router mode will block broadcasts while it is not transparent.

Device supports Multicast packet pass-through in Router mode. Router can act as DHCP server and use Network Address Translation (Masquerading) feature which is widely used by the Access Points. NAT will act as the firewall between LAN and WLAN networks. Additional Firewall settings can be configured for Layer 3 packet filtering and access control in Router mode.

Bridge Mode

Bridge Mode Network Settings

In bridge mode the device forwards all the network management and data packets from one network interface to the other without any intelligent routing. For simple applications this provides efficient and fully transparent network solution. WLAN (wireless) and LAN (Ethernet) interfaces belong to the same network segment which has the same IP address space. WLANand LAN interfaces form the virtual bridge interface while acting as the bridge ports. The bridge has assigned IP settings for management purposes:

Bridge IP Address:

The device can be set for static IP or can be set to obtain an IP address fromthe DHCP server it is connected to. One of the IP assignment modes must be selected:

DHCP : choose this option to assign the dynamic IP address, Gateway and DNS address by the local DHCP server.

STATIC : choose this option to assign the static IP settings for the bridge interface.

IP Address: enter the IP address of the device while Static Bridge IP Address mode is selected. This IP will be used for the device management purposes.

IP Address and Netmask settings should consist with the address space of the network segment where device resides. If the device IP settings and administrator PC (which is connected to the device in wired or wireless way) IP settings will use different address space, the device will become unreachable.

Netmask: This is a value which when expanded into binary provides a mapping to define which portions of IP address groups can be classified as host devices and network devices.

Netmask defines the address space of the network segment where device resides. 255.255.255.0 (or /24) Netmask is commonly used among many C Class IP networks.

Gateway IP: Typically, this is the IP address of the host router which provides the point of connection to the internet. This can be a DSL modem, Cable modem, or aWISP gateway router.

Device will direct the packets of data to the gateway if the destination host is not within the local network. Gateway IP address should be from same address space (on same network segment) as the device.

Primary/Secondary DNS IP:

The Domain Name System (DNS) is an internet "phone book" which translates domain names to IP addresses. These fields identify the server IP addresses of where the device looks for the translation source.

Primary DNS server IP address should be specified for the device management purposes.

Secondary DNS server IP address is optional. It is used as the fail-over in case the primary DNS server will become unresponsive.

DHCP Fallback IP:

In case the Bridge is placed in Dynamic IP Address mode (DHCP) and is unable to obtain an IP address from a valid DHCP server, it will fall back to the static IP address listed here. In case the IP settings of the devices are unknown, they can be access with the help of the *UConfig utility*.

The *UConfig Utility* should be started on the administrator PC which resides on the same network segment as the device.

Device will return to the default IP configuration (192.168.168.1/255.255.255.0) if the *Reset to defaults* routine is initiated.

Spanning Tree Protocol:

Multiple interconnected bridges create larger networks using the IEEE 802.1d Spanning Tree Protocol (STP), which is used for finding the shortest path within network and to eliminate loops fromthe topology.

If the STP is turned on, the Bridge device will communicate with other network devices by sending and receiving Bridge Protocol Data Units (BPDU). STP should be turned off (selected by default) when the device is the only bridge on the LAN or when there are no loops in the topology as there is no sense for the bridge to participate in the Spanning Tree Protocol in this case.

Bridge mode Firewall Configuration Settings

Firewall functionality on bridge interface can be enabled using the "Enable Firewall" option.

Bridge Firewall rules can be configured, enabled or disabled while using Firewall configuration window which is opened with the "Configure" button.

Firewall entries can be specified by using the following criteria:

Interface the interface (WLAN or LAN) where filtering of the incoming/passing-through packets is processed;

IP Type sets which particular L3 protocol type (ICMP, TCP, UDP, P2P) should be filtered;

Source IP/mask is the source IP of the packet (specified within the packet header), usually it is the IP of the host system which sends the packets;

Source Port is the source port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which sends the packets;

Destination IP/mask is the destination IP of the packet (specified within the packet header), usually it is the IP of the system which the packet is addressed to;

Destination Port is the destination port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which the packet is addressed to.

Comments is the informal field for the comment of the particular firewall entry. Few words about the particular firewall entry purpose are saved there usually.

On flag enables or disables the effect of the particular firewall entry. All the added firewall entries are saved in systemconfiguration file, however only the enabled firewall entries will be active during the system operation.

New Firewall entries can be saved by activating Apply button or discarded by activating Cancel button in the Firewall configuration window.

All the active firewall entries are stored in the FIREWALL chain of the ebtables filter table, while the device is operating in Bridge mode.

Click Apply Setting and Save Changes button to save the changes made in the Network page.

Appendix II Wireless with Router Mode

This section provides more details on wireless with router function.

The role of the LAN andWLAN interface will change accordingly to the **Wireless Mode** while the device is operating in **Router** mode:

Wireless interface and all the wireless clients connected are considered as the internal LAN and the Ethernet interface is dedicated for the connection to the external network while the device is operating in AP/APWDS wireless mode;

Wireless interface and all the wireless clients connected is considered as the external network and the all the network devices on LAN side as well as the Ethernet interface itself is considered as the internal network while the device is operating in Station/Station WDS mode.

Wireless/wired clients are routed from the internal network to the external one by default. Network Address Translation (NAT) functionality works the same way.

AP-Router mode Network Settings

IP Address: This IP addresses represents the LAN or WLAN interface which is connected to the internal network according to the wireless operation mode described above. IP will be used for routing in internal network (it will be the Gateway IP for all the devices connected on the internal network). IP address also will be used for the management purpose of the device.

WLAN IP Address: This IP addresses represents the LAN orWLAN interface which is connected to the external network according to the wireless operation mode described above. This is the IP address can be used for the routing and the device management purposes. The external network interface can be set for static IP or can be set to obtain an IP address from the DHCP server which should reside in the external network. One of the IP assignment modes must be selected for the external network interface:

DHCP choose this option to obtain the IP address, Gateway and DNS address dynamically from the external DHCP server.

PPPoE choose this option to obtain the IP address, Gateway and DNS address dynamically fromthe external PPPoE server.

Static choose this option to assign the static IP settings for the external interface.

IP Address and Netmask settings should consist with the address space of the network segment where the device resides. If the device IP settings and administrator PC (which is connected to the device through wired or wireless) IP settings will use different address space, the device will become unreachable.

Netmask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks, which support IP address range 192.0.0.x to 223.255.255.x. ClassC network Netmask uses 24 bits to identify the network (alternative notation "/24") and 8 bits to identity the host.

Gateway IP: This is the IP address of the host router which resides on the external network and provides the point of connection to the next hop towards the internet. This can be a DSLmodem, Cable modem, or aWISP gateway router. The device will direct all the packets to the gateway if the destination host is not within the local network.

Gateway IP address should be fromthe same address space (on the same network segment) as the device's external network interface (Wireless interface in the Station case and the LAN interface in the AP case).

Primary/Secondary DNS IP: The Domain Name System(DNS) is an internet "phone book" which translates domain names to IP addresses. These fields identify the server IP addresses where the DNS requests are forwarded by the device.

Primary DNS server IP ismandatory. It is used by the DNS Proxy and for the device management purpose.

Secondary DNS server IP address is optional. It is used as the fail-over in case the primary DNS server will become unresponsive.

Enable NAT: Network Address Translation (NAT) enables packets to be sent from the wired network (LAN) to the wireless interface IP address and then sub-routed to other client devices residing on it's local network while the device is operating in AP/APWDS wireless mode and in the contrariwise direction in "Station/StationWDS" mode.

NAT is implemented using the masquerade type firewall rules. NAT firewall entries are stored in the iptables nat table, while the device is operating in Router mode. Please refer to the iptables tutorial for detailed description of the NAT functionality in Router mode.

Static routes should be specified in order the packets should pass-through the based device if the NAT is disabled in while operating in Router network mode.

Enable DHCP Server: Dynamic Host Configuration Protocol (DHCP) Server assigns IP addresses to clients which will associate to the wireless interface while the device is operating in AP/APWDS wireless mode and assigns IP addresses to clients which will connect to the LAN interface while the device is operating in Station/StationWDS mode.

Range Start/End: This range determines the IP addresses given out by the DHCP server to client devices on the internal network which use dynamic IP configuration.

Lease Time: The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interrupt, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more slight interruptions to the client while it will acquire new IP addresses fromthe DHCP server.

DHCP Fallback IP: In case the external network interface of the Router is placed in Dynamic IP Address mode (DHCP) and is unable to obtain an IP address from a valid DHCP server, it will fall back to the static IP address listed here. In case the IP settings of the device are unknown, they can be retrieved with the help of the UConfig utility and should be started on the administrator PCwhich resides on the same network segment as the device.

Port Forwarding Settings

Port Forwarding: Port forwarding allows specific ports of the hosts residing in the internal network to be forwarded to the external network. This is useful for number of applications such as FTP servers, gaming, etc. where different host systems need to be seen using a single common IP address/port. Port Forwarding rules can be set in Port Forwarding window, which is opened by enabling the Port Forwarding option and activating the Configure button.

Port Forwarding entries can be specified by using the following criteria:

Private IP is the IP of the host which is connected to the internal network and needs to be accessible from the external network;

Private Port is the TCP/UDP port of the application running on the host which is connected to the internal network. The specified port will be accessible from the external network;
Type is the L3 protocol (IP) type which needs to be forwarded from the internal network.
Public Port is the TCP/UDP port of the based device which will accept and forward the connections from the external network to the host connected to the internal network.
Comments is the informal field for the comment of the particular port forwarding entry.
Few words about the particular port forwarding entry purpose are saved there usually.
Enabled flag enables or disables the effect of the particular port forwarding entry.
All the added firewall entries are saved in systemconfiguration file, however only
the enabled port forwarding entries will be active during the system operation.
New entries in port forwarding can be saved by activating Save button or discarded by activating

DNS Proxy: The DNS Proxy forwards the Domain Name System requests from the hosts which reside in the internal network to the DNS server while device is in operating in Router mode. Valid Primary DNS Server IP needs to be specified for DNS Proxy functionality. Internal network interface IP of the device should be specified as the DNS server in the host configuration in order DNS Proxy should be able to get the DNS requests and translate domain names to IP addresses afterwards.

Bridge mode Firewall Configuration Settings

Firewall functionality on any router interface can be enabled using the "Enable Firewall" option.
Router Firewall rules can be configured, enabled or disabled while using Firewall
configuration window which is opened with the "Configure" button.
Firewall entries can be specified by using the following criteria:

Interface the interface (WLAN, LAN or PPP) where filtering of the incoming/passing-through packets is processed;

IP Type sets which particular L3 protocol type (ICMP, TCP, UDP, P2P) should be filtered;
Source IP/mask is the source IP of the packet (specified within the packet header), usually it is the IP of the host system which sends the packets;
Source Port is the source port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which sends the packets;
Destination IP/mask is the destination IP of the packet (specified within the packet header), usually it is the IP of the system which the packet is addressed to;
Destination Port is the destination port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which the packet
is addressed to.
Comments is the informal field for the comment of the particular firewall entry. Few words about the particular firewall entry purpose are saved there usually.
On flag enables or disables the effect of the particular firewall entry. All the added firewall entries are saved in systemconfiguration file, however only the enabled firewall entries

will be active during device operation.

New entries in Firewall can be saved by activating Apply Setting and Save Changes button or discarded by activating Cancel button in the Firewall configuration window.

All the active firewall entries are stored in the FIREWALL chain of the iptables filter table, while the device is operating in Router mode.

PPPoE: Point-to-Point Protocol over Ethernet (PPPoE) is a virtual private and secure connection between two systems which enables encapsulated data transport. It is commonly used as the medium for subscribers to connect to Internet Service Providers. Select the IP Address option PPPoE to configure a PPPoE tunnel in order to connect to an ISP.

Only the external network interface can be configured as PPPoE client as all the traffic will be sent via this tunnel. The IP address, Default gateway IP and DNS server IP address will be obtained from the PPPoE server after PPPoE connection is established. Broadcast address is used for the PPPoE server discovery and tunnel establishment.

Valid authorization credentials are required for the PPPoE connection:

PPPoE Username username to connect to the server (must match the configured on the PPPoE server);

Password password to connect to the server (must match the configured on the PPPoE server);

PPPoE MTU/MRU the size (in bytes) of the Maximum Transmission Unit (MTU) and MaximumReceive Unit (MRU) used for the data encapsulation while transferring it through the PPP tunnel;

Enable DMZ: The Demilitarized zone (DMZ) can be enabled and used as a place where services can be placed such asWeb Servers, Proxy Servers, and E-mail Servers such that these services can still serve the local network and are at the same time isolated fromit for additional security. DMZ is commonly used with the NAT functionality as an alternative for the Port Forwarding while makes all the ports of the host network device be visible fromthe external network side.

DMZ Management Port: Web Management Port for the based device (TCP/IP port 80 by default) will be used for the host device if DMZ Management Port option is enabled. In this case device will respond to the requests from the external network as if it was the host which is specified with DMZ IP. It is recommended to leave Management Port disabled while the based device will become inaccessible fromthe external network if enabled.

DMZ IP: connected to the internal network host, specified with the DMZ IP address will be accessible from the external network.

With a multicast design, applications can send one copy of each packet and address it to the group of computers that want to receive it. This technique addresses packets to a group of receivers rather than to a single receiver. It depends on the network to forward the packets to the hosts which need to receive them. Common Routers isolate all the broadcast (thus multicast) traffic between the internal and external networks, however provides the multicast traffic pass-through functionality.

Click Change button to save the changes made in the Network page.

Appendix III- Advanced Settings

This section provides more detail explanation on advanced setting for routing and wireless settings.
The Advanced options page allows you to manage advanced settings that influence on the device performance and behavior. The advanced wireless settings are dedicated for more technically advanced users who have a sufficient knowledge about wireless LAN technology. These settings should not be changed unless you know what effect the changes will have on your device.

Advanced Wireless Setting

The 802.11 data rates include 1, 2, 5.5, 11 Mbps for IEEE 802.11b mode and 6, 9, 12, 18, 24, 36, 48, 54Mbps for IEEE 802.11a/g mode. The Rate Algorithmhas a critical impact on performance in outdoor links as generally lower data rates are more immune to noise while higher rates are less immune, but are capable of higher throughput.

Rate Aggressiveness :
Allows user to reduce or increase transmit rate while still remain in Fully Auto Algorithm. There are 2 scenarios that Rate Aggressiveness is useful. Environment might be noisy at times. Lower the throughput will ensure better stability. Rate Aggressiveness allows device to reduce the transmit rate, so range or power can be higher. Choose a range of value from -3,-2,-1.
Environment might be free of interference. But the fully auto algorithm might give low throughput. Increase Rate Aggressiveness will increase transmit rate in this case to get higher throughput. Choose a range of value from +3, +2, +1.

Noise Immunity option increases the robustness of the device to operate in the presence of noise disturbance which is usually generated by external 802.11 traffic sources, channel hopping signals and other interferers.

RTS Threshold: determines the packet size of a transmission and, through the use of an access point, helps control traffic flow. The range is 0-2347bytes, or word off . The default value is 2347 which means that RTS is disabled.
RTS/CTS (Request to Send / Clear to Send) is the mechanism used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden terminal problem.
RTS/CTS packet size threshold is 0-2347 bytes. If the packet size the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. If the packet size is equal to or less than threshold the data frame gets sent immediately.
Systemuses Request to Send/Clear to Send frames for the handshake which provide collision reduction for access point with hidden stations. The stations are sending a RTS frame first while data is send only after handshake with an AP is completed. Stations respond with the CTS frame to the RTS which provides clear media for the requesting station to send the data. CTS collision control management has time interval defined during which all the other stations hold off the transmission and wait until the requesting station will finish transmission.

Fragmentation Threshold: specifies the maximumsize for a packet before data is fragmented

into multiple packets. The range is 256-2346 bytes, or word off . Setting the Fragmentation Threshold too lowmay result in poor network performance.
The use of fragmentation can increase the reliability of frame transmissions. Because of sending smaller frames, collisions are much less likely to occur. However lower values of the Fragmentation Threshold will result lower throughput as well. Minor or no modifications of the Fragmentation Threshold value is recommended while default setting of 2346 is optimumin most of the wireless network use cases.

Station Isolation: This option allows packets only to be sent from the external network to the CPE and vice verse (applicable for AP/APWDS mode only). If the Client Isolation is enabled wireless stations connected to the same AP will not be able to interconnect on both layer 2 (MAC) and layer 3 (IP) level. This is effective for the associated stations and WDS peers also.

Acknowledgement Timeout

Device has an auto-acknowledgement timeout algorithm which dynamically optimizes the frame acknowledgement timeout value without user intervention. This is a critical feature required for stabilizing long-distance outdoor links. The user also has the ability to enter the value manually.
Distance: specify the distance value in miles (or kilometers) using slider or enter the value

manually. The signal strength and throughput falls off with range. Changing the distance value will change the ACK Timeout to the appropriate value of the distance.

ACK Timeout: specify the ACK Timeout. Every time the station receives the data frame it sends an ACK frame to the AP (if transmission errors are absent). If the station receives no ACK frame fromthe AP within set timeout it re-sends the frame. The performance drops because of the too many data frames are re-send, thus if the timeout is set too short or too long, it will result poor connection and throughput performance.
Changing the ACK Timeout"== value will change the Distance to the appropriate distance value for the ACK Timeout.

Auto: Adjust control and enable the ACK Timeout Self-Configuration feature. If enabled, ACK Timeout value will be derived dynamically using an algorithmsimilar to the Conservative Rate Algorithm described above. It is not recommended to use Auto Adjust option for long range links if the signal level is lowor the high level of interference is present.
If two or more stations are located at the considerably different distance fromthe Access Point, the highest ACK Timeout for the farthest station should be set at the AP side. It is not recommended to use Auto Adjust option for Point-to-Multipoint connections as it will not warrant highest network performance in all the use cases.

Signal Strength LED Settings

LED Thresholds Configuration

The LED's for signal strength on the device can be made to light on when received signal levels reach the values defined in the following fields. This allows a technician to easily deploy a CPE without logging into the unit (i.e. for antenna alignment operation).

Signal LEDThresholds specify the marginal value of Signal Strength (dBm) which will switch on LEDs indicating signal strength:

LED 1 (Red) will switch on if the Signal Strength reaches the value set in an entry field next to it.
LED 2 (Yellow) will switch on if the Signal Strength reaches the value set in an entry field next to it.
LED 3 (Green) will switch on if the Signal Strength reaches the value set in an entry field next to it.
LED 4 (Green) will switch on if the Signal Strength reaches the value set in an entry field next to it.

Configuration example: if the Signal Strength fluctuates around RSSI 15-30, the LED Thresholds can be adjusted to the RSSI values 15, 20, 25, 30.

Appendix IV- Services

This section provides more details on the systemmanagement services.

Ping WatchDog

The ping watchdog sets the device to continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, the device will automatically reboot. This option creates a kind of "fail-proof" mechanism.
PingWatchdog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. The Ping works by sending ICMP echo request packets to the target host and listening for ICMP echo response replies. If the defined number of replies is not received, the tool reboots the device.
Enable Ping Watchdog: control will enable PingWatchdog Tool.
IP Address To Ping: enter the target host IP address to monitor.
Ping Interval: specify time interval (in seconds) between to send the ICMP echo requests .
Startup Delay: specify initial time delay (in seconds) fromdevice startup or reboot to start sending first ICMP echo requests . Minimumvalue is 60 seconds.
Failure Count To Reboot: specify the number of ICMP echo response replies. If the specified number of ICMP echo response packets is not received continuously, the PingWatchdog Tool will reboot the device.

SNMP Agent

Simple Network Monitor Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. Device contains an SNMP agent which allows it to communicate to SNMP manage applications for network provisioning.
SNMP Agent provides an interface for device monitoring using the Simple Network Management

Protocol (an application layer protocol that facilitates the exchange of management information between network devices). SNMP Agent allows network administrators to monitor network performance, find and solve network problems. For the purpose of equipment identification, it is always a good idea to configure SNMP agents with contact and location information:

Enable SNMP Agent: control will enable SNMP Agent.

SNMP Community: specify SNMP community string. It is required to authenticate access to MIB objects and functions as embedded password. The device supports a Read-only community string that gives read access to authorized management stations to all the objects in the MIB except the community strings, but does not allow write access for device that supports SNMP v1.
Contact: specify the identity or contact in case an emergency situation arise.
Location: specify the physical location of the device.

NTP Client, Web, Telnet, SSH Server

NTP Client: The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. It can be used to set the device system time. SystemTime is reported next to the every System Log entry while registering system events if Log option is enabled.
Web Server: the following the deviceWeb Server parameters can be set there:
Use Secure Connection (HTTPS): If checkedWeb server will use secure HTTPS mode. HTTP mode is selected by default.

Secure Server Port: Web Server TCP/IP port setting while using HTTPS mode.
Server Port: Web Server TCP/IP port setting while using HTTP mode.
Telnet Server: the following the device Telnet Server parameters can be set there:
Enable Telnet Server: Enables Telnet access to the device.
Server Port: Telnet service TCP/IP port setting.
SSH Server: the following the device SSH Server parameters can be set there:
Enable SSH Server: Enables SSH access to the device.
Server Port: SSHservice TCP/IP port setting.

SystemLog

Enable Log : option enables the registration routine of the systemlog messages.
Enable Remote Log enables the syslog remote sending function while Systemlog messages are sent to a remote server specified by the Remote Log IP Address and Remote Log Port.
Remote Log IP Address is the host IP address where syslog messages should be sent. Remote host should be configured properly to receive syslog protocol messages.
Remote Log Port is the TCP/IP port of the host syslog messages should be sent. "514" is the default port for the commonly used systemmessage logging utilities
.
Every logged message contains at least a *System Time* and a Host Name. Usually a particular service name which generates the system event is specifies also within the message. Messages from different services have different context and different level of the details. Usually *error*, *warning* or *informational*

systemservices messages are reported. Themore detailed systemmessages are reported, the greater volume of log messages will be generated.

Copyright